DEFENCE **R&D** DÉFENSE

Biometric Data Safeguarding Technologies Analysis and Best Practices
Study Report

Raj Nanavati
International Biometric Group

The scientific or technical validity of this Contract Report is entirely the responsibility of the Contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada.

Canadä

Biometric Data Safeguarding Technologies Analysis and Best Practices
Study Report

Prepared by:
International Biometric Group

Scientific Authority:
Pierre Meunier
DRDC Centre for Security Science

The scientific or technical validity of this Contract Report is entirely the responsibility of the Contractor and the contents do not necessarily have the approval or endorsement of Defence Research and Development Canada.

Defence R&D Canada – Centre for Security Science

Principal Author

Raj Nanvati International Biometric Group

Approved by

Original signed by [Approved by Name]

Jack Pagotto

DRDC CSS Section Head

Approved for release by

Original signed by [Released by Name]

Dr. Mark Williamson

DRDC CSS DDG-DRP Chair

Contents

Figures and Tables

Executive Summary

Biometric Data Safeguarding Technologies Analysis and Best Practices International Biometric Group DRDC CSS CR 2011-29 December 2011

Background

This document is the Study Report for PSTP 02-0351BIO, **Biometric Data Safeguarding Technologies Analysis and Best Practices**. One of the main goals of the Public Security Technical Program (PSTP) Biometrics Community of Practice is to evaluate, analyze, and implement biometric technologies that enhance national capabilities in access control, identity verification, and e-Commerce security in a manner that is consistent with Canadian laws and acts. This is done in collaboration with the appropriate Government of Canada agencies and departments responsible for national security, border control and security, and law enforcement and immigration.

The Lead Federal Department for the Study is Canada Border Services Agency (CBSA). Additional partners include the following:

- Royal Canadian Mounted Police
- Transport Canada
- Defence Research and Development Canada (DRDC) – Toronto
- Office of the Information and Privacy Commissioner of Ontario
- University of Toronto
- Indiana University-Purdue University Indianapolis (IUPUI)
- IBG-Canada

The rapid progress of biometrics technology in the last few years and the ease with which biometrics data can be acquired has resulted in the accumulation of large varying databases of biometrics information. This trend will continue in the future, with databases growing at an ever-increasing rate. The purpose of the Study is to examine some of the issues surrounding the sharing and safeguarding of biometric data in the Canadian Public Security context writ large. Throughout the study, the modality focus will be on iris biometrics (prime focus) and fingerprints (secondary).

Biometric privacy enhancing technologies (PETs) are among the most promising technologies for data safeguarding. These technologies leverage biometric information to improve and ensure personal privacy while protecting sensitive information and assets. PETs can be categorized as follows:

- **Untraceable Biometrics** – defined by Dr. Ann Cavoukian, Ontario Privacy Commissioner, as a new class of emerging privacy enhancing technologies such as biometric encryption
- **Anonymous Biometrics** – a system where biometric data are not connected to any personal data; biometric data can be taken to another system to connect with personal information
- **Revocable ("Private") Biometrics** – allow people to have multiple biometric identities using the same biometric information; identities can be used independently or anonymously

This document presents methodologies and results from scientific studies that identify and evaluate biometric technologies with respect to their ability to be used securely (in terms of safeguarding biometric databases). These new biometric technologies and associated data safeguarding capabilities must be consistent with the Government of Canada's dual prosperity and security mandates, and must consider legal, ethical, cultural, and privacy issues.

Biometric Data Sharing and Safeguarding Considerations

The scale and complexity of biometric samples gathered by national and international systems are increasing and

becoming widespread. The current maturity level of biometrics has facilitated the use of biometrics in a wide range of government applications, while much work remains in devising acceptable ways of controlling the use, storage, and exchange of biometric data and personal information.

Privacy threats related to biometrics have been discussed extensively. Major privacy risk areas are described as followed:

- The ability to cross match data subjects across different services or applications by comparing biometric templates.
- The possibility to extract sensitive information from the stored biometric data
- The extension of application scope of biometric technology outside consent of the owner

The various security threats associated with data sharing and safeguarding can be described by potential attacks on various components of a biometric systems, including during biometric data capture, storage, and transmission. Key security concepts related to data safeguarding include confidentiality, integrity, and revocability.

Confidentiality ensures that information is not disclosed to unauthorized entities. In a biometric system, biometric data is stored and transmitted between various subsystems. Both storage and transmission of data should be protected against eavesdropping, unauthorized disclosure or modification of the data. This requires cryptographic techniques such as biometric encryption, or symmetric or asymmetric ciphers.

Integrity is the property of safeguarding the accuracy and completeness of assets in a given dataset. If the integrity of a biometric reference or the result of the various processing algorithms and subsystems are untrustworthy, the verification outcome will also be untrustworthy. Cryptographic means to protect the integrity of the data, such as signatures or authenticated encryption and time stamping, are required.

A strong security concern for biometric system relates to **revocability** and renewability of biometric templates. Individuals have a limited number of irises and fingers; identity theft renders corresponding biometric template as unusable for future use. Due to the persistence of biometric characteristics, a compromised biometric template is compromised forever. The risk of compromised templates can be mitigated for certain types of attacks by providing methods to allow renewable biometric templates.

Modality-Specific Considerations

Fingerprint, face recognition, and iris recognition are among the primary modalities considered for use in data safeguarding applications.

Fingerprint: Strengths	Fingerprint: Weaknesses
- Proven technology capable of high accuracy - Performance (accuracy, throughput) of leading technologies is well-documented and understood - Ability to enroll multiple fingers; exceptionally high accuracy for ten print collections - Ergonomic, easy-to-use devices - Fingerprint data is almost universally interoperable, facilitating searches against watchlists	- Performance can deteriorate over time - Association with forensic applications - Users can intentionally damage fingerprints, reducing performance - Implementation of large-scale systems requires highly specialized expertise for performance tuning and optimization

Face Recognition: Strengths	Face Recognition: Weaknesses
- Does not require user training or effort - Can often leverage existing image datasets and existing photograph processes - Capable of identification at a distance - Capable of rapid 1:N identification with relatively little	- Susceptible to high false non-match rates in 1:1 and 1:N applications - Changes in acquisition environment reduce matching accuracy - Changes in physiological characteristics reduce matching accuracy

processing power • Performance improves hand-in-hand with camera quality and image resolution	• Lighting, camera angle reduce matching accuracy
Iris Recognition: Strengths	**Iris Recognition: Weaknesses**
• Exceptionally resistant to false matching • Default operation is identification mode • High stability of characteristic over lifetime • Hands-free operation • Real-time searches against large datasets (e.g. 10m irises) are possible with modest CPU loads	• Acquisition of iris image requires more training and attentiveness than most biometrics • User discomfort with eye-based technology • Glasses can impact performance • Propensity for false non-matching or failure to capture

Select Biometric Data Safeguarding Implementations

The rapid advancement of biometric technology along with the ease with which biometrics data can be acquired has resulted in the accumulation of large datasets of biometrics information. However, reporting of best practices has been minimal in regards to data sharing and safeguarding. Critical areas assessed in this Study include system requirements, risk factors, strengths and weaknesses of the deployed data safeguarding technologies, privacy issues, and performance. The objective is to provide deployers and decisions-makers with the full range of information necessary to implement secure and interoperable solutions in defence and security applications. Implementations analyzed are an follows:

Border / Traveler Systems	Civil ID / Criminal ID	Surveillance
• U.S. Visitor and Immigration Status Indicatory Technology • EURODAC • Japan Biometrics Identification System • The Five Country Conference Protocol • CANPASS • NEXUS	• Gambia Biometric identification System • The Bangladesh Voter Registration Project • National ID Card (Thailand) • Multilingual Automated Registration System (United States)	• New Delhi Railway Station Face Recognition Surveillance (India) • Community Protection Face Recognition System (United Arab Emirates)

Biometric PET Approaches

The study reviews the following biometric PET techniques.

- Fuzzy Cryptosystems
- Homomorphic Encryption
- Local Aggregation
- Multifactor Key Generation
- Noninvertible Transforms
- Parametric Key Generation
- Random Projection

Fuzzy Cryptosystems

A "sketch" or "vault" is a secured template whose development can be traced to the "fuzzy vault" scheme proposed by Juels and Sudan. The scheme was designed to encrypt data such that it could be unlocked by similar but inexact matches. Variants of the fuzzy vault scheme are referred to more generally as fuzzy cryptosystems. The method lent itself well to the protection of biometric templates, where inputs are inconsistent due to lighting, rotation, etc. The mechanism for obfuscating data in fuzzy cryptosystems is to insert random noise that resembles genuine minutiae points or other features. In doing so an attacker cannot easily differentiate genuine features and false features. Most variations of this system follow key release protocols, though some generate keys from the biometric data. Fuzzy cryptosystems are perhaps the most practiced and debated template protection methods in academia. As a result there is a wealth of literature on the security vulnerabilities and countermeasures to mitigate these vulnerabilities,

making this method among the most mature of all template protection methods despite its many shortcomings.
Homomorphic Encryption

An encryption method is homomorphic if the structure of the ciphertext is preserved in the encryption of the plaintext. Homomorphism has a "malleable" property, meaning that the ciphertext can be converted into another ciphertext that also reverts to the original plaintext. Homomorphic encryption can be used to calculate the similarity between an input templates and stored templates in the encrypted domain, preventing servers from extracting sensitive information from a query. Many of the proposed homomorphic encryption methods make use of existing cryptosystems proposed by Paillier, Goldwasser-Micali, and ElGamal, all of which are semantically secure protocols. Homomorphic encryption may be applied to one step in the template protection processes.

Local Aggregation

Local aggregation is a means of extracting features from a biometric input by counting the number of features that appeared within the confines of many randomly generated regions superimposed the input. Each element in the set contains the number of features found in one of the randomly superimposed regions. Regions are generated according to a secret key that is unique to every user. This implies that each user has a unique but repeatable pattern of random regions. If someone were to present a stolen image without its corresponding key, features would be counted incorrectly and the imposter would be invalidated. Templates produced by this method can be cancelled by reenrolling the biometric with a different key, resulting in a new pattern of random regions. The method is considerably tolerant to intraclass variations because it checks only for the presence of features within wide regions. Intraclass variations due to minor rotation, translation, and warping are not likely to push the features outside the boundaries of the regions as long as the input is aligned. Cryptographic keys are computed from metrics like the number of minutiae points within each region, which are easier to reproduce in subsequent transactions than the exact coordinates and angles of the minutiae points. Overall this method possesses the advantage of computational simplicity. Furthermore, because this approach does not transform the biometric features, it avoids producing inadvertent errors due to arbitrarily or unreliably designed transform functions.

Multifactor Key Generation

Multifactor key generation combines a biometric with one or more other inputs, such as a password or token, to produce cryptographic keys. This approach is essentially a form of salting, whereby the user supplies secret auxiliary information that influences the transformation of the biometric image or template. Combining biometrics with other authentication factors has proven to be a reliable means of generating secure templates or cryptographic keys. From a security perspective, this method is advantageous because it combines something that the user 'is' with something that the user 'has' or 'knows'. The principal tradeoff for security in multifactor key generation protocols is usability, not necessarily verification performance. Access control systems that use multifactor key generation could easily become a hassle to users who forgot their password or token. Furthermore, the need to present multiple inputs during authentication is impractical for applications like security checkpoints.

Noninvertible Transforms

Noninvertible transforms are a generic means of obfuscating biometric template data by way geometric transformation. Transforms are executed either at the single domain or the feature domain. The literature has favored feature domain transforms, which alter features such as the position of the minutiae coordinates. By contrast, single domain transforms alter the pixels of the raw image. Figure 23 illustrates the manner in which minutiae points are repositioned by a feature domain geometric transform. The dots indicate the position and angle of fingerprint minutiae. Observe how they are repositioned after a Gaussian transform. Any template protection method could employ a noninvertible transform as one of several means of obfuscating the template data. Typically the parameters which influence the transform are used as the cancelable property in a protected template. For additional security, these parameters can be derived from a user-supplied input such as a password or a private key.

Parametric Key Generation

Parametric key generation methods classify biometric features according to predefined parameters and generate a key derived from the parameter outputs rather than from the template itself. This approach mitigates the problem of intraclass variations because the shape and position of the features do not influence the construction of the encrypted

template. For example, rather than store the locations of minutiae points, a fingerprint is classified simply as having an arch, loop, or whorl. Many parameters must be defined to ensure uniqueness among templates. The performance of any parametric key generation algorithm depends on the reliability of its parameters. A parameter is considered to be reliable if it consistently returns the same value upon many presentations of the same biometric. Therefore the best performing algorithms are likely to contain many parameters with simple definitions, allowing for many possible combinations and accurately reproduced queries.

Random Projection

Random projection is a means of reducing the dimensionality of a set of points while nearly preserving the distances between the points. Some template protection methods use random projection as a means to randomly map minutiae coordinates while preserving semantic meaning in final set.

Iris Recognition Assessments and Performance Evaluations

Iris recognition technology is considered a candidate for use in biometric PETs due to the richness and stability of data in iris images. To gauge the suitability of this modality for use in PETs, Indiana University-Purdue University Indianapolis (IUPUI) analyzed previous studies of iris recognition performance and conducted a new study of iris recognition performance.

Assessment of Iris Recognition through Variable-Quality Iris Datasets: Methodology

IUPUI evaluated the ability of a commercial iris recognition algorithm to process 7 iris image datasets. Matching was performed on a 1:1 basis at the default 1:1 threshold.

Dataset Name	Image Format & Volume	Quality / Capture Notes
Iris Challenge Evaluation (ICE)	640x480 , 2953 images	Controlled environment, cooperative subjects, illuminated in the near infra-red (NIR) range
Chinese Academy of Sciences (CASIA) 2.0	640x480 , 2400 images	NIR
CASIA 3.0 Set 1	320x280 , 2639 images	NIR; captured in two sessions, > one month interval
CASIA 3.0 Set 2	640x480 , 16213 images	NIR; captured in one session
CASIA 3.0 Set 3	640x480 , 3183 images	NIR; captured in one session
West Virginia University	640x480 , 1852 images	NIR; noisy, heterogeneous data, with obstructions, inconsistent illumination, out-of-focused, off-angle irises
UBIRIS	800x600 , 1877 images	Color images acquired in visible wavelengths; Two distinct sessions, images are predominately frontal gaze,
Multimodal Biometric Grand Challenge (MBGC)	2048x2048 , 148 videos, 1 second duration	NIR; focal length of IOM is 2~3 feet, images acquired while subjects walked toward the camera, primarily frontal view, subjects instructed to look at iris cameras
IUPUI multi-wavelength	1280x1024 , 352 videos	NIR; obtained from both eyes on two separate occasions, time period between each data acquisition is at least one week, only used green wavelength to test
IUPUI Remote	1280x1024 , 731 videos, 30 fps	NIR; average iris radius was 95 pixels, data was acquired in two sessions, at least one week between sessions, 6 videos per iris, variety of positions and situations

ICE database UBIRIS database

CASIA V2.0 MBGC database

CASIA V3.0 IUPUI Multi-wavelength (green)

WVU database IUPUI Remote database

Assessment of Iris Recognition through Variable-Quality Iris Datasets: Results and Analysis

Metrics used to evaluate performance were quality, false rejection rate (FRR), false acceptance rate (FAR), and failure to process rate (FTPR). Results are shown in the charts below.

Dataset-Based Iris Recognition Accuracy

Failure to Process Rates
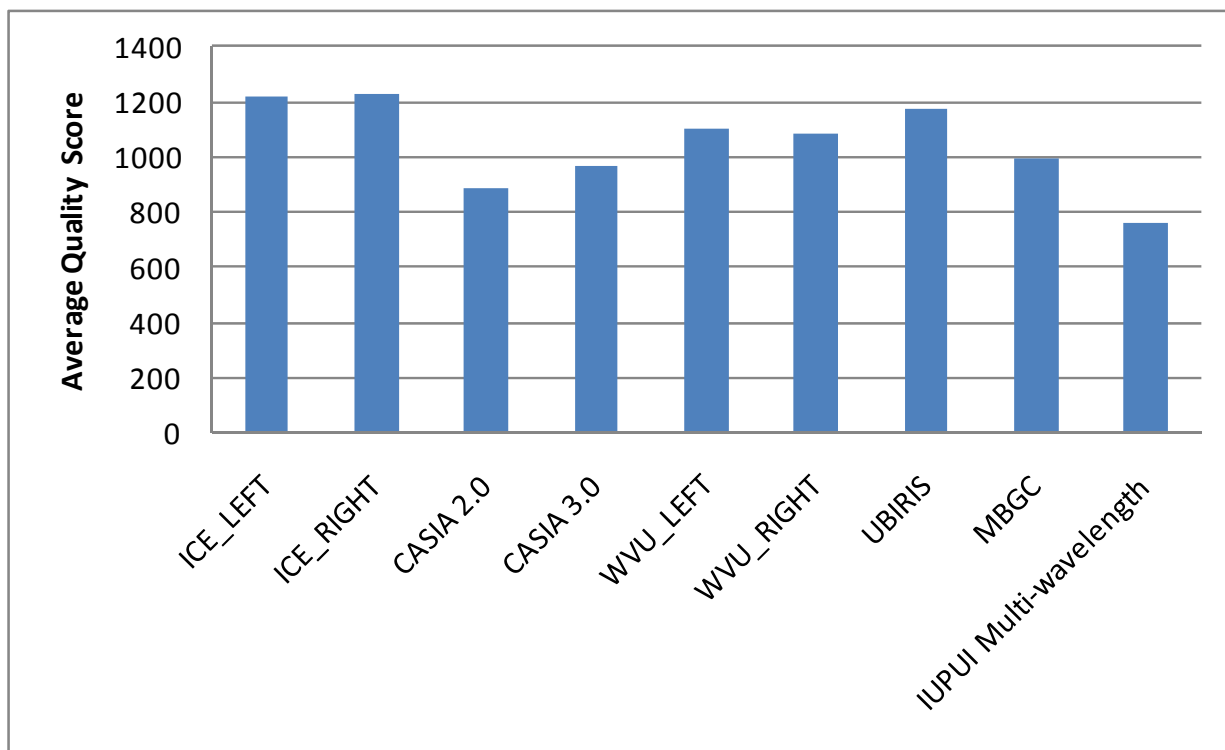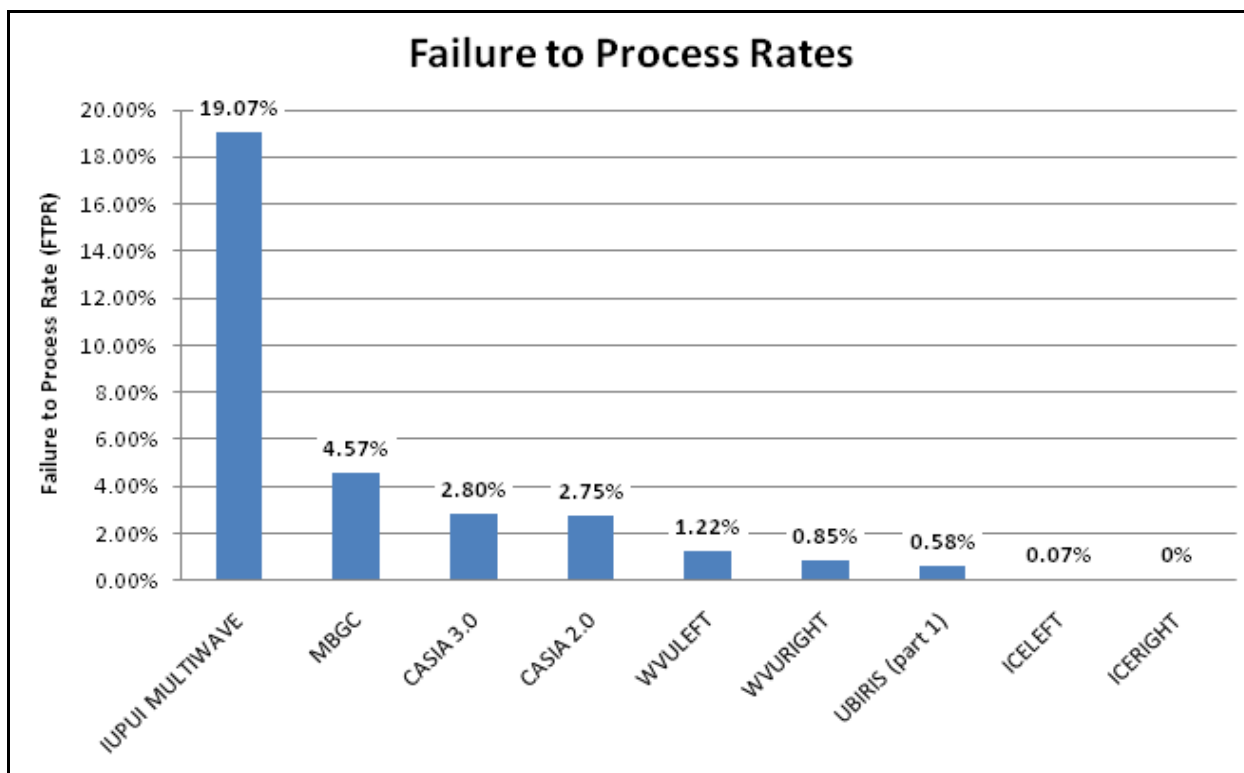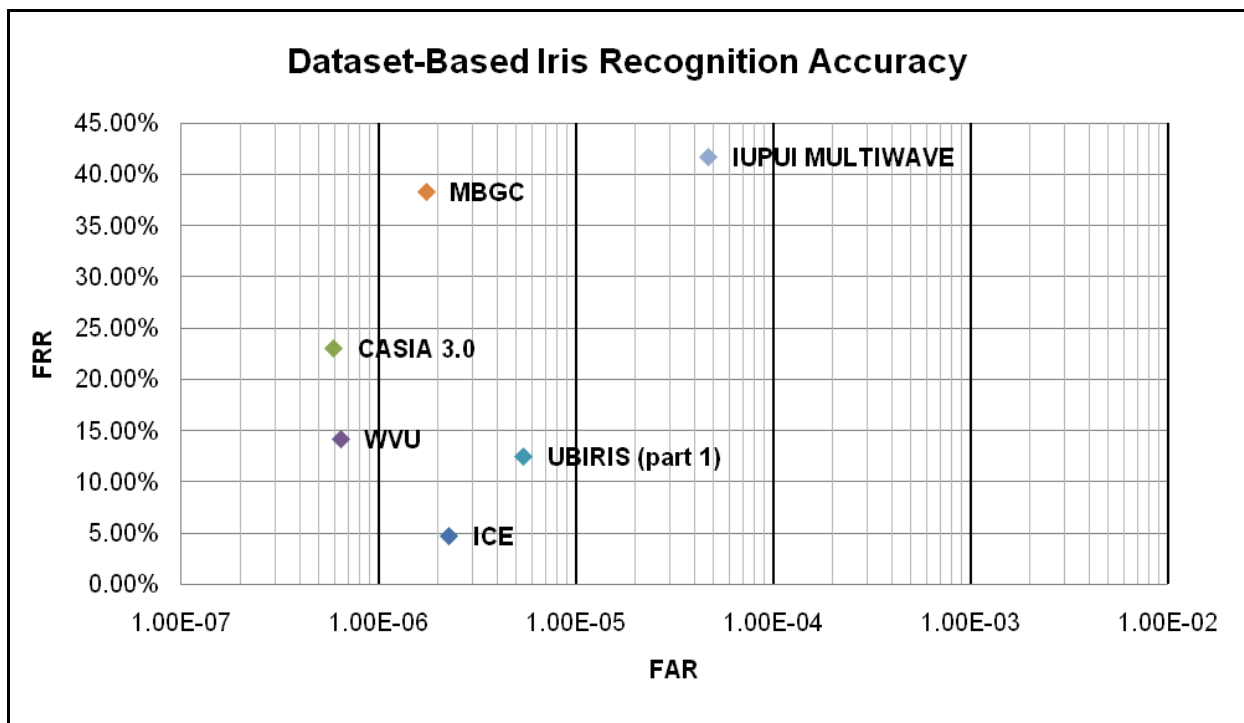
The following conclusions can be drawn from this multi-dataset evaluation:

- Processing and matching are very fast. The system can perform iris recognition in 17.8ms (including segmentation, feature extraction and 1:1 matching).
- It has very low FAR when using a decision threshold (Hamming Distance) of 0.33. The HD used for large-scale identification would have resulted in a 0.00% FAR and higher FRR for all datasets.
- The system is capable of processing visible wavelength images, assuming that iris patterns are good enough for recognition.
- The system can work reasonably well with regular pupil dilation.

Areas for improvement include the following:

- The system is unable to process non-cooperative, off-angle iris images.
- Since the commercialized system is designed for images acquired from a specific, paired acquisition system, preferences in iris image resolution and illumination are present. Usually, the commercialized system can work best with iris images with resolution about 200 pixels across the iris. However, for lower resolution or higher resolution images, if resolution can be adjusted properly without deforming iris patterns, the system can also perform accurate iris recognition.
- Recognition accuracy is affected dramatically by illumination condition, contrast, and motion blur.
- The commercialized system would not work with dark color iris images in visible wavelength due to the lack of recognizable iris patterns.
- Hamming Distances are not necessarily symmetric. When used for enrollment, lower-quality images resulted in higher (worse) HDs.

Impact of Compression on Iris Recognition

Data compression is beginning to play a part in the use of iris recognition systems. In the field applications using handheld iris recognition devices often use wireless communication to connect to the central server for identification and verification. While it will be ideal to have wide bandwidth for transmission in real-life applications, it often needs to transmit captured images or templates over a narrow-bandwidth communication channel. In this case, minimizing the amount of data to transmit (which is possible through compression) minimizes the time to transmit, and saves energy. The study analyzes previously-conducted evaluations on compression techniques including region on interest compression.

Iris Recognition with Contact Lenses

Contact lenses with iris patterns printed on them can cause errors in the iris recognition system. Experts have studied the effect of transparent contact lens on the recognition accuracy of several iris recognition systems. Their data was taken in the same studio with consistent ambient indoor lighting. They visually inspected all the images and reject any that were low quality. They then classified the contact-lens wearing subjects into five different categories based on a visible inspection they preformed manually.
12,003 iris images from 87 contact-lens-wearing subjects and 9,697 non-contact-lens wearing subjects then processed through 3 matching algorithms. Contact-lens wearing were subjects grouped into five different categories based on a visible inspection they preformed manually.

Category 0	No contact lens
Category 1	Minimal or no change to the iris. At most these images contain a faint visible edge.
Category 2	Images contain a definite circular boundary on the iris area.
Category 3	Contains images which the lens has writing on the lens, the lens fits improperly causing it not to lay flat on iris, or the lens produces an artifact.
Category 4	Contains the iris images where the subject is wearing hard contact lenses. Hard contacts produce a very noticeable ring and severely distort the area they cover.

Results below illustrate slight false reject rate (FRR) increases across categories 0-3 then substantial increases in FRR for category 4.
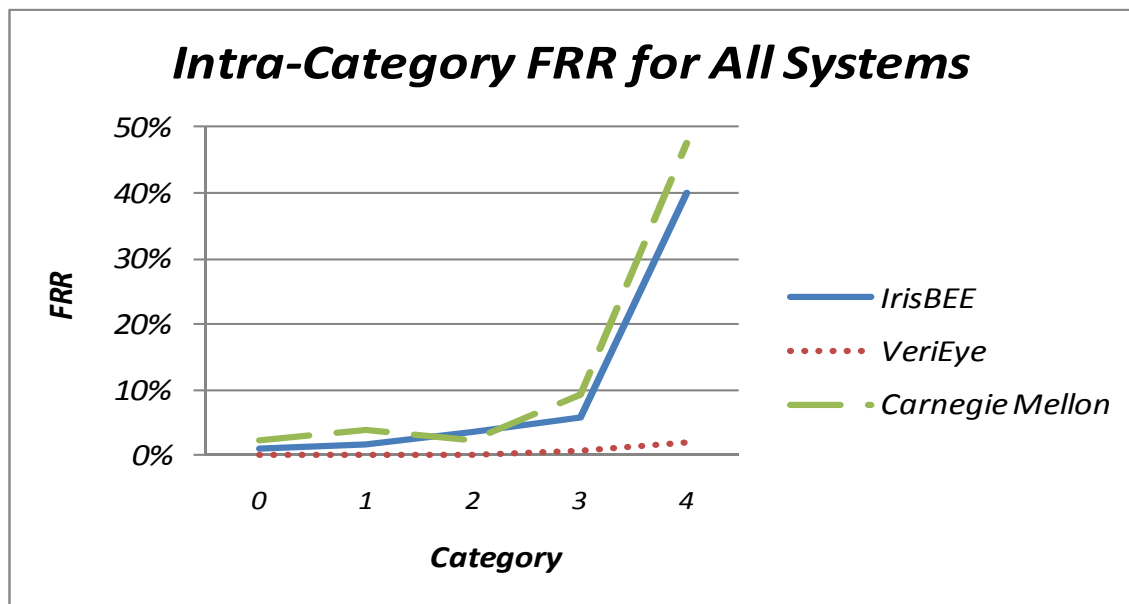
Intra-Category FRR for All Systems

Video-based Non-cooperative Iris Recognition

As iris recognition technologies continues to mature, it will gain the ability to acquire an image without the end user even knowing. This will make iris recognition a great way to verify people because it will cause no extra burden for the user. This technology also has great potential for finding people of interest, because a non-cooperative iris recognition system can identify people without the making the person aware they are being indentified. This application is particularly valuable for security at airport, borders or any other any public place.

Multiple Wavelength Based Iris Recognition

NIR images have been dominant in iris identification. One downside to NIR light is it requires active NIR illumination. Visible wavelength iris recognition could function using environmental illumination. In addition, visible wavelength recognition is important because it can be used with facial recognition for multimodal biometrics. In the future regular color surveillance camera may have the capability to perform iris recognition. Visible wavelength iris recognition has its own challenges, especially it is challenging for dark color eyes and remote iris recognition. In the future, multiple-wavelength iris recognition may attack more attention and can work with multiple-wavelength face recognition together for video surveillance.

Multimodal Eye Recognition

Since the iris patterns of dark color eyes could reveal rich and complex patterns only under NIR light, if the NIR iris image be obtained in long distance, the accuracy of iris recognition will drop dramatically. And if we acquire iris image in visible light, the iris patterns of dark color eyes will be hardly visible under visual light. The sclera, the white and opaque outer protective covering of the eye, can also be used in human identification. The sclera image segmentation process, it includes image down-sampling, conversion to the HSV color space, estimation of the sclera region, iris and eyelid detection, eyelid and iris boundary refinement, mask creation, and mask up-sampling. The sclera region is estimated using the best representation between two color-based techniques.

GenKey Fingerprint-Based PET Performance Evaluation

GenKey Technology

GenKey, a leading provider of biometric PET solution, has developed a biocryptic algorithm that bridges cryptology with biometrics. This patented algorithm converts a biometric image into Public Key Infrastructure (PKI)-compatible crypto keys that are irreversible and share no mathematical relationship with the biometric sources they represent. Its solutions can be applied to a variety of contexts including education, licensing and healthcare. The GenKey algorithm provides a means to enroll and verify individuals based on biometric information, such as a fingerprint. The algorithm offers a number of options which provide tradeoffs between recognition speed, accuracy, and biometric privacy.

GenKey Feature Template vs. ID Key Enrollments

The GenKey algorithm can perform two types of enrollment. In feature template enrollment, discriminating features from fingerprint images are extracted and stored as the individual's biometric template. The feature template is stored for later use and the biometric image may be discarded. ID Key enrollment also extracts discriminating

features from fingerprint images, but converts features into a numerical value which represents the individual's biometric. At the conclusion of an ID Key

enrollment, the ID Key (numerical value) is stored and the biometric image and feature template may be discarded. This type of enrollment is focus of IBG's performance evaluation.

IBG tested two GenKey ID Key types:

- **Standard ID Key**s offer performance near the performance of the feature template enrollments.
- **Flex ID Key**s tradeoff key size and accuracy.

IBG evaluated performance using the Standard ID Key as well as 12, 25, 56, and 107-byte Flex ID keys.

	Feature Template (not a PET)	**Standard ID Key (PET)**	**Flex ID Key (PET)**
Accuracy	Feature enrollments provide the most robust performance.	Standard ID Keys will perform at only slightly degraded error rates as compared to feature templates.	Flex ID Keys provide a range of accuracy performance options. Larger Flex ID Keys provide accuracy similar to Standard ID Keys.
Privacy	Offers some privacy protection for the fingerprint; having access to a feature template does not provide a malicious user with capability to reconstruct the original fingerprint. With detailed knowledge of the GenKey feature template creation process, a malicious user could gain access to general information about the fingerprint structure.	ID Keys offer a privacy advantage over feature template enrollment. A malicious user with access to the ID Key cannot practically regenerate the fingerprint features or extract any detailed information about the fingerprint structure. The technique used to convert the feature template to a key is analogous to a cryptographic one-way function. It is easy to compute an ID Key from a feature template; however, reversing this process is computationally infeasible.	
Throughput	Feature enrollments offer the fastest search speeds. The GenKey algorithm is capable of performing millions of feature template matches per second using ordinary computer hardware.	While not as fast as feature template matching, ID Key verifications can also be performed at relatively high speeds using ordinary computer hardware; GenKey estimates rates of hundreds of thousands of verifications per second. Match speed increases (i.e. becomes slower) as stricter match thresholds are applied.	
Typical Key Size	128-256 bytes	64-128 bytes	12-107 bytes

GenKey Test Data

IBG used a collection of approximately 6000 flat fingerprint images (left and right index) from 1200 subjects collected under indoor office conditions. Fingerprint images were collected through a 500dpi Cross Match Verifier. Each subject provided two samples per position during a first visit. Additionally, approximately 650 of the 1,200 subjects provided two samples per position during a second visit which occurred roughly one month after the first.

GenKey Enrollment and Recognition Processes

Using a Software Development Kit (SDK) provided by GenKey, IBG developed a custom application that performed feature extraction, template creation, and ID Key creation. Both index fingerprints had to enroll in order for an enrollment to be successful. IBG also developed a custom application that performed bulk matching. Second-visit fingerprint images were used for recognition (i.e. as probe images) are compared against first-visit fingerprint data.
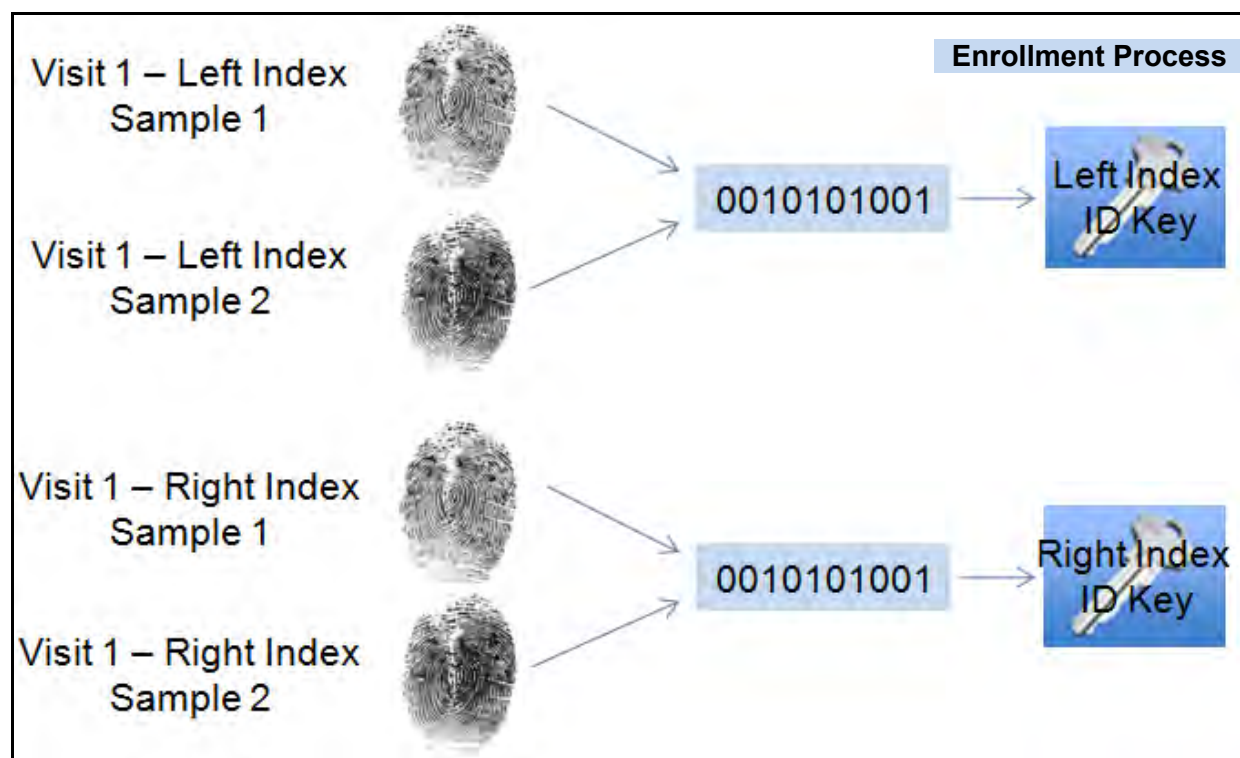
In addition to processing through the GenKey algorithm, IBG processed the same fingerprint dataset through a widely-adopted, minutiae-based fingerprint algorithm –Neurotechnology VeriFinger version 6.3. The VeriFinger processing approach was equivalent to the GenKey approach described below. Comparing and contrasting GenKey results with VeriFinger results will provide a general frame of reference for validating the commercial viability of GenKey's ID Key technology.
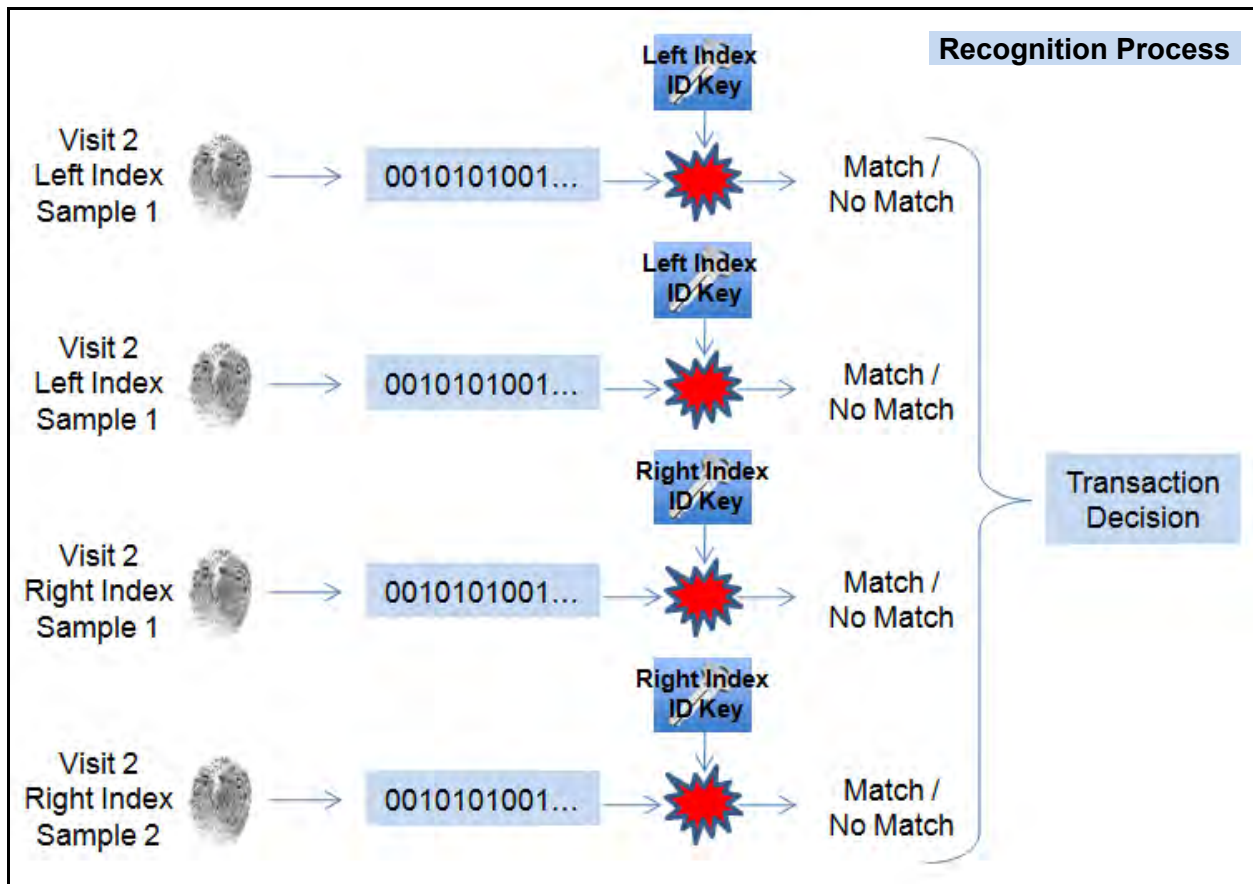
Processing volumes are shown below.

	GenKey	VeriFinger 6.N
Subjects	650	650
Genuine comparisons	456	459
Impostor Comparisons	550976	560741

GenKey Test Results

Based on collection and comparison processes described above, the following metrics were generated.

Usability Metrics	Accuracy Metrics
• Failure to Encode Rate (FTE) • Failure to Acquire Rate (FTA) • Processing Time	• False Match Rate (FMR) • False Non-Match Rate (FNMR) • Distribution of Errors by Subject

Failure to Enroll	Enrollment Attempts	FTE Count	FTE Rate
VeriFinger 6.3	2448	42	1.72%
GenKey ID Key	2448	45	1.84%

Failure to Acquire	Recognition Encoding Attempts	FTA Count	FTA Rate
VeriFinger 6.3	1841	1	0.05%
GenKey ID Key	1841	66	3.59%

Results show that GenKey and Verifinger FTE are roughly equivalent, while GenKey FTA is substantially higher

than VeriFinger FTA. This underscores the concept that GenKey is predicated on the use of high-quality images whose quality is validated in real time at the point of capture.
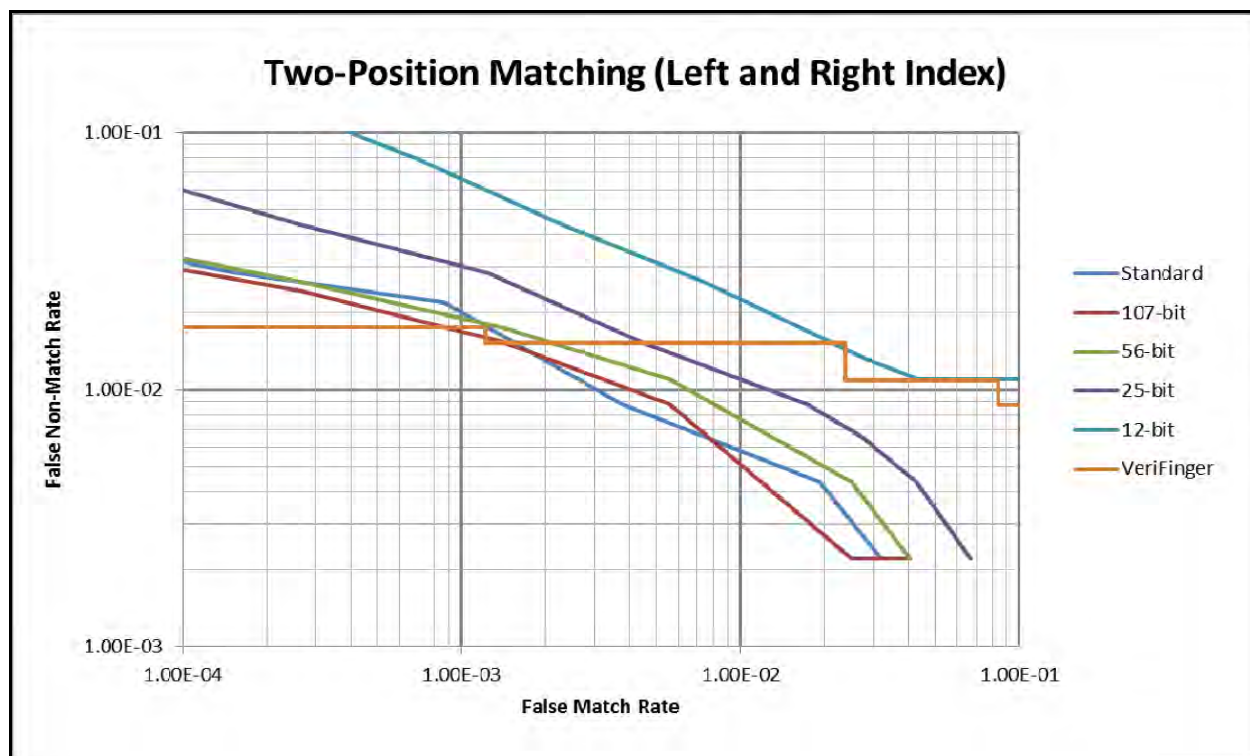
Comparative performance assessment with a challenging dataset demonstrates the viability of commercial, fingerprint-based DETs. Biometric PET performance is relatively close to that of a widely-deployed, NIST-tested minutiae-based matcher

For many biometric systems, certain subjects encounter higher false match rates than others. IBG analyzed the distribution of false matches across subjects. Subject-specific false match rates (aggregated across all evaluated ID Key types and sizes, and measured at a typical threshold of 0.45) ranged from as high as 4.04% and as low as 0.00%. While false match rates generally decline as key sizes increase, in some cases subjects encountered higher false match rates at larger key sizes. For example, 251 of 457 subjects encountered higher false match rates at an ID Key size of 56 bytes than at 25 bytes.

Conclusions

The following high-level conclusions can be drawn from this study.

- Aspects of non-cooperative iris recognition performance, including high failure to enroll and false non-match rates, complicate its use as a PET
- Controlled iris recognition capture, and/or high-quality iris images, will increase the likelihood of iris usage as a PET
- Comparative performance assessment with a challenging dataset demonstrates the viability of commercial, fingerprint-based DETs
- GenKey performance is close to that of a widely-deployed, NIST-tested minutiae-based matcher
- Deployers should study how to incorporate key-based approaches into their application architectures

Sommaire

Analyse et meilleures pratiques relatives aux technologies de protection des données biométriques. **International Biometric Group RDDC CSS CR 2011-29 Décembre 2011**

Contexte

Le présent document constitue le Rapport d'étude PSTP09-0351BIO, **Analyse et meilleures pratiques relatives aux technologies de protection des données biométriques**. L'un des principaux objectifs du Programme technique de sécurité publique (PTSP) de la Communauté de praticiens en biométrie est d'évaluer, d'analyser et de mettre en application des technologies biométriques qui améliorent les capacités du pays en matière de contrôle de l'accès, de la vérification de l'identité et de la sécurité de commerce électronique tout en respectant les lois et les actes canadiens. Ces mesures sont prises en collaboration avec les agences et ministères du gouvernement canadien responsables de la sécurité nationale, du contrôle frontalier et de sécurité à la frontière, avec la police et les services d'immigration.

Le ministère fédéral en chef pour la présente étude est l'Agence des services frontaliers du Canada (ASFC). D'autres partenaires comprennent :

- Gendarmerie royale du Canada
- Transports Canada
- Recherche et développement pour la Défense Canada (RDDC) – Toronto
- Commissariat à l'information et à la protection de la vie privée de l'Ontario
- Université de Toronto
- Indiana University-Purdue University Indianapolis (IUPUI)
- IBG-Canada

L'évolution rapide des technologies biométriques des dernières années et la facilité avec laquelle les données biométriques peuvent être acquises ont mené à une accumulation de vastes bases de renseignements biométriques divers. Cette tendance se maintiendra étant donné le rythme constant avec lequel les bases de données sont alimentées. L'objectif de la présente étude est d'examiner certaines questions relatives au partage et à la protection des données biométriques dans le contexte de la sécurité publique au Canada. Au cours de l'étude, l'accent sera placé sur les données biométriques de l'iris (point principal) et les empreintes digitales (point secondaire).

Les technologies d'amélioration de la confidentialité des données biométriques (ACDB) sont parmi les technologies les plus prometteuses en matière de protection des données. Ces technologies misent sur les renseignements biométriques pour améliorer et assurer la protection des renseignements personnels tout en protégeant des renseignements et des biens sensibles. Ces technologies peuvent être classées comme suit :

- **Données biométriques non retraçables** – définies par Madame Ann Cavoukian, commissaire à la protection de la vie privée de l'Ontario, comme une nouvelle catégorie de technologies d'amélioration de la vie privée émergentes comme le cryptage des données biométriques
- **Données biométriques anonymes** – système où les données biométriques ne sont pas reliées à des données personnelles; les données biométriques peuvent être placées dans un autre système afin de les relier à des renseignements personnels
- **Données biométriques révocables (privées)** – permet à certaines personnes d'obtenir de multiples identificateurs biométriques en utilisant les mêmes renseignements biométriques; les identificateurs peuvent être utilisés indépendamment ou de manière anonyme

Le présent document introduit des méthodologies et les résultats d'études scientifiques qui identifient et évaluent les technologies biométriques sur leur capacité à être utilisées de manière sécurisée (en terme

de protection des bases de données biométriques). Ces nouvelles technologies biométriques et les capacités de protection de données connexes doivent être conformes aux mandats de prospérité et de sécurité du gouvernement canadien et doivent prendre en considération les questions relatives au droit, à l'éthique, à la culture et à la protection des renseignements personnels.

Points à considérer en matière de partage et de protection des données biométriques

La quantité et la complexité des échantillons de données biométriques recueillis par les systèmes nationaux et internationaux s'accroissent et se propagent. Le niveau de maturité actuel des données biométriques a facilité l'utilisation de celles-ci dans un vaste éventail d'applications gouvernementales, bien qu'il reste beaucoup de travail à faire dans la mise au point de moyens acceptables pour contrôler l'utilisation, le stockage et l'échange de données biométriques et de renseignements personnels.

Les menaces relatives à la protection des données biométriques ont été examinées de manière approfondie. Les principaux secteurs de risque pour la protection de la vie privée sont décrits ainsi :

- La capacité de trouver la compatibilité croisée de personnes visées pour divers services ou diverses applications en comparant les matrices de données biométriques.
- La possibilité d'extraire des renseignements sensibles des données biométriques stockées.
- L'extension de l'étendue d'une technologie biométrique à l'extérieur du cadre de consentement du propriétaire

Les diverses menaces de sécurité associées au partage et à la protection des données peuvent être décrites par des attaques potentielles sur divers éléments des systèmes biométriques, y compris la saisie, le stockage et la transmission des données biométriques. Les concepts de sécurité clés relatifs à la protection des données comprennent la confidentialité, l'intégrité et la révocabilité.

La **confidentialité** permet d'assurer que les renseignements ne sont pas dévoilés à des personnes non autorisées. Dans un système biométrique, les données sont stockées dans divers sous-systèmes et transmises entre ceux-ci. Le stockage et la transmission des données devraient être protégés contre l'interception clandestine, la divulgation non autorisée ou la modification de données. Cela nécessite des techniques cryptographiques comme le cryptage biométrique ou symétrique ou les cryptages asymétriques.

L'**intégrité** constitue la protection de la précision et de l'intégralité des biens dans un ensemble de données. Si l'intégrité d'une référence biométrique ou le résultat des divers traitements d'algorithme et sous-systèmes ne sont pas dignes de foi, le résultat de la vérification ne sera pas de digne de foi également. La cryptographie signifie protéger l'intégrité des données comme les signatures, le cryptage authentifié et l'horodatage.

Une des questions importantes en matière de protection des systèmes biométriques touche la **révocabilité** et la renouvelabilité des gabarits de données biométriques. Chaque individu possède un nombre limité d'iris et de doigts et donc, le vol d'identité rend le gabarit biométrique correspondant inutilisable. En raison de la longévité des caractéristiques biométriques, un gabarit biométrique compromis le sera pour toujours. Il est possible d'empêcher certains types d'attaques de compromettre les gabarits grâce à des méthodes de création de gabarits de données biométriques renouvelables.

Modalités spécifiques à prendre en considération

Les empreintes digitales, la reconnaissance du visage et la reconnaissance de l'iris sont parmi les modalités primaires prises en considération pour les applications de protection des données.

Empreintes digitales : forces	Empreintes digitales : faiblesses
- Technologie éprouvée et d'une grande précision - Le rendement (précision, débit) des technologies de	- Le rendement peut diminuer avec le temps - Association avec des applications judiciaires

pointe est bien documenté et compris • Capable de traiter plusieurs doigts à la fois; précision exceptionnellement grande pour la collecte de 10 empreintes • Dispositifs ergonomiques et faciles à utiliser • Les données sur les empreintes sont presque toutes interexploitables, ce qui facilite les recherches dans des listes de surveillance	• Les utilisateurs peuvent endommager intentionnellement les empreintes, ce qui réduit le rendement • La mise en application de systèmes à grande échelle nécessite une expertise hautement spécialisée pour régler et optimiser le rendement

Reconnaissance de visage : forces	Reconnaissance de visage : faiblesses
• Ne nécessite pas de formation et ne requiert pas d'effort pour l'utilisateur • Peut souvent avoir une incidence sur les ensembles de données d'images existants et les processus de photographie existants • Capable d'une identification à distance • Capable d'une identification 1:N rapide qui ne nécessite qu'une faible capacité de traitement • Le rendement s'améliore grâce à la qualité de la caméra et à la résolution d'image	• Susceptible à des taux élevés de fausse non-correspondance dans les applications 1:1 et 1:N • Des changements dans l'environnement d'acquisition diminuent la précision des correspondances • Des changements dans les caractéristiques physiologiques réduisent la précision des correspondances • L'éclairage et l'angle de la camera réduisent la précision des correspondances
Reconnaissance de l'iris : forces	Reconnaissance de l'iris : faiblesses
• Extrêmement résistante aux fausses correspondances • Fonctionne par défaut en mode d'identification • Grande stabilité des caractéristiques pour la durée de vie • Fonctionnement mains libres • Des recherches en temps réel dans de vastes ensembles de données (p. ex. : 10 millions d'iris) sont possibles avec des charges CPU légères	• L'acquisition d'une image de l'iris nécessite plus de formation et d'attention que la plupart des autres données biométriques. • Malaise de l'utilisateur pour les technologies qui font appel aux yeux • Le port de lunettes peut avoir une incidence sur le rendement. • Propension pour de fausses non-correspondances ou incapacité de saisir les données

Mises en application de systèmes de protection des données biométriques

Les avancées rapides des technologies biométriques de même que la facilité avec laquelle les données biométriques peuvent être acquises ont mené à une accumulation de vastes ensembles de données biométriques. Cependant, les rapports portant sur les meilleures pratiques relatives au partage et à la protection des données sont peu nombreux. Les secteurs critiques évalués dans la présente étude comprennent les exigences du système, les facteurs de risques, les forces et les faiblesses des technologies de protection des données déployés, les questions relatives à la protection de la vie privée et le rendement. L'objectif est de fournir aux personnes chargées du déploiement et des décisions une panoplie de renseignements nécessaires pour mettre en place des solutions sécurisées et interexploitables pour les applications de défense et de sécurité. Les mises en application analysées sont :

Systèmes frontière / voyageur	Identification civil / indentification criminel	Surveillance
• U.S. Visitor and Immigration Status Indicatory Technology • EURODAC • Japan Biometrics Identification System • The Five Country Conference Protocol • CANPASS • NEXUS	• Gambia Biometric identification System • The Bangladesh Voter Registration Project • National ID Card (Thaïlande) • Multilingual Automated Registration System (États-Unis)	• New Delhi Railway Station Face Recognition Surveillance (Inde) • Community Protection Face Recognition System (Émirats arabes unis)

Approches des techniques ACDB

L'étude examine les techniques ACDB suivantes :

- Systèmes cryptographiques flous
- Chiffrement homomorphique
- Rassemblement local
- Génération de clé multifactorielle
- Transformations sans inversion
- Génération de clé paramétrique
- Projection aléatoire

Systèmes cryptographiques flous

Une « esquisse » ou « enceinte » est un gabarit sécurisé dont l'élaboration peut être reliée au projet « enceinte floue » proposé par Juels et Sudan. Ce projet a été conçu pour chiffrer des données de telle manière qu'elles pourraient être déverrouillées par des correspondances semblables, mais inexactes. Généralement, on appelle « systèmes cryptographiques flous » les diverses versions du projet enceinte floue. La méthode se prête bien à la protection de gabarits biométriques dans lesquels les entrées sont irrégulières en raison de l'éclairage, de la rotation, etc. Le mécanisme de masquage des données dans les systèmes cryptographiques flous consiste à insérer un bruit aléatoire qui ressemble à des points caractéristiques ou autres caractéristiques authentiques. De cette manière, l'attaquant ne peut facilement différencier les caractéristiques authentiques des fausses caractéristiques. La plupart des versions de ce système respectent les protocoles clés de libération, bien que certaines génèrent des clés à partir des données biométriques. Les systèmes cryptographiques flous sont peut-être les méthodes de protection de gabarit les plus utilisées et les plus controversées dans le milieu universitaire. Par conséquent, il existe une panoplie de documents écrits sur la vulnérabilité relative à la sécurité et aux contre-mesures pour atténuer celles-ci, faisant de cette méthode, malgré ses nombreuses faiblesses, l'une des plus raisonnées de toutes les méthodes de protection de gabarit.

Chiffrement homomorphique

Une méthode de chiffrement est homomorphique si la structure du cryptogramme est conservée dans le chiffrement du texte en clair. L'homomorphisme possède une caractéristique « malléable », c'est-à-dire que le cryptogramme peut être convertit en un autre cryptogramme, lequel renvoie au texte en clair original. Le chiffrement homomorphique peut être utilisé pour calculer la ressemblance entre des gabarits de données d'entrée et des gabarits stockés dans le domaine du chiffrement, ce qui empêche les serveurs d'extraire des renseignements sensibles lors d'une interrogation. Plusieurs des méthodes de chiffrement homomorphiques proposées utilisent des systèmes de chiffrements existants proposés par Paillier, Goldwasser-Micali et ElGamal et elles constituent toutes des protocoles sémantiquement sécurisés. Le chiffrement homomorphique peut être utilisé pour une étape des processus de protection des gabarits.

Rassemblement local

Le rassemblement local sert à extraire des caractéristiques d'une donnée biométrique en comptant le nombre de caractéristiques qui apparaissent à l'intérieur de plusieurs régions générées aléatoirement et superposées à la donnée. Chaque élément de cet ensemble comprend le nombre de caractéristiques retrouvées dans une des régions superposées aléatoirement. Les régions sont générées selon une clé secrète unique à chaque utilisateur. Cela signifie que chaque utilisateur possède un regroupement reproductible de régions aléatoires. Si quelqu'un présentait une image volée sans posséder la clé correspondante, les caractéristiques seraient comptées incorrectement et l'imposteur serait invalidé. Les gabarits générés par cette méthode peuvent être annulés en réinscrivant la donnée biométrique à l'aide d'une autre clé, ce qui permet de former un nouveau regroupement de régions aléatoires. Cette méthode

tolère très bien les variances intraclasses, car elle vérifie uniquement la présence de caractéristiques au sein de larges régions. Les variances intraclasses engendrées par une faible rotation, un petit déplacement et une petite déformation ne devraient pas faire sortir les caractéristiques des limites des régions tant et aussi longtemps que la donnée est alignée. Les clés cryptographiques sont calculées avec le système métrique comme le nombre de points caractéristiques de chaque région. En effet, les caractéristiques sont plus faciles à reproduire dans les transactions subséquentes que les coordonnées et les angles exacts des points caractéristiques. Sur l'ensemble, cette méthode possède l'avantage de la simplicité computationnelle. De plus, étant donné que cette approche ne transforme pas les caractéristiques des données biométriques, elle ne produit pas d'erreurs involontaires causées par des fonctions de transformations conçues arbitrairement ou de manière peu fiable.

Génération de clé multifactorielle

La génération de clé multifactorielle combine une donnée biométrique et une autre ou d'autres données d'entrée comme un mot de passe ou un jeton d'authentification, pour produire des clés cryptographiques. Cette approche est, essentiellement, une forme de « salage » dans lequel l'utilisateur fournit un renseignement auxiliaire secret qui a une incidence sur la transformation de l'image biométrique ou du gabarit. La combinaison de données biométriques et d'autres facteurs d'authentification s'est prouvée un moyen fiable de générer des gabarits ou des clés cryptographiques sécurisés. D'une perspective de sécurité, cette méthode est avantageuse, car elle combine quelque chose que l'utilisateur « est » à quelque chose que l'utilisateur « possède » ou « connaît ». Le principal compromis en matière de sécurité avec les protocoles de génération de clé multifactorielle est la convivialité, pas nécessairement le rendement de vérification. Les systèmes de contrôle de l'accès qui utilisent la génération de clé multifactorielle pourraient facilement devenir contrariants pour les utilisateurs qui oublient leur mot de passe ou leur jeton d'authentification. De plus, le besoin d'entrer de multiples données pendant l'authentification est impraticable pour les applications comme les points de contrôle de sûreté.

Transformations sans inversion

Les transformations sans inversion sont un moyen générique de masquer les données du gabarit biométrique grâce à la transformation géométrique. Les transformations sont effectuées soit dans le domaine unique ou l'espace des attributs. La documentation favorise les transformations de l'espace des attributs, lesquelles modifient les caractéristiques comme la position des coordonnées caractéristiques. Par contre, les transformations du domaine unique modifient les pixels de l'image brute. La Figure 23 illustre la manière avec laquelle les points caractéristiques sont repositionnés grâce à une transformation géométrique de l'espace des attributs. Les points indiquent la position et l'angle des caractéristiques d'une empreinte digitale. On peut remarquer comment ils sont repositionnés après une transformation Gaussian. Toute méthode de protection de gabarit pourrait utiliser une transformation sans inversion comme moyen de masquer les données du gabarit. Typiquement, les paramètres qui ont une incidence sur la transformation sont utilisés comme propriété révocable dans un gabarit protégé. Pour une sécurité accrue, ces paramètres peuvent être empruntés à une donnée fournie par l'utilisateur comme un mot de passe ou une clé privée.

Génération de clé paramétrique

Les méthodes de génération de clé paramétrique classent les caractéristiques biométriques conformément aux paramètres prédéfinis et génèrent une clé issue des données de sortie du paramètre plutôt que du gabarit. Cette approche atténue le problème des variances intraclasses puisque la forme et la position des caractéristiques n'ont pas d'incidence sur la construction du gabarit chiffré. Par exemple, plutôt que de stocker les emplacements des points caractéristiques, une empreinte digitale est classée selon son arche, sa boucle ou son tourbillon. De nombreux paramètres doivent être définis pour assurer son unicité parmi les gabarits. Le rendement de tout algorithme de génération de clé paramétrique dépend de la fiabilité de ses paramètres. Un paramètre est considéré fiable s'il obtient toujours la même valeur lorsqu'on lui présente la même donnée biométrique. Les algorithmes les plus efficaces comprennent fort probablement de nombreux paramètres et des définitions simples, permettant de nombreuses combinaisons et des interrogations reproduites avec précision.

Projection aléatoire

La projection aléatoire est un moyen de réduire la dimensionnalité d'un ensemble de points tout en préservant les distances entre ces points. Certaines méthodes de protection des gabarits utilisent la projection aléatoire comme moyen pour tracer aléatoirement les coordonnées caractéristiques tout en préservant la signification sémantique dans l'ensemble final.

Évaluation de la reconnaissance de l'iris et évaluation du rendement

La technologie de reconnaissance de l'iris est considérée une technologie candidate pour les technologies ACDB en raison de la richesse et de la stabilité des données relatives aux images de l'iris. Pour jauger la pertinence de cette modalité dans les technologies ACDB, l'Indiana University-Purdue University Indianapolis (IUPUI) a analysé des études antérieures relatives au rendement de la reconnaissance de l'iris et a mené une nouvelle étude sur ce rendement.

Évaluation de la reconnaissance de l'iris par le biais des ensembles de données sur des iris variable-qualité : méthodologie

L'IUPUI a évalué la capacité d'un algorithme de reconnaissance de l'iris commercial de traiter sept (7) ensembles de données d'images d'iris. La correspondance a été effectuée sur une base 1:1 à un seuil de défaillance de 1:1.

Nom de l'ensemble de données	Format et volume de l'image	Notes qualité/saisie
Iris Challenge Evaluation (ICE)	640 x 480, 2 953 images	Environnement contrôlé, sujets coopératifs, éclairé dans le proche infrarouge (NIR)
Chinese Academy of Sciences (CASIA) 2.0	640 x 480, 2 400 images	NIR
CASIA 3.0 Set 1	320 x 280, 2 639 images	NIR; saisie en deux sessions, > d'un mois d'intervalle
CASIA 3.0 Set 2	640 x 480, 16 213 images	NIR; saisie en une session
CASIA 3.0 Set 3	640 x 480, 3 183 images	NIR; saisie en une session
West Virginia University	640 x 480, 1 852 images	NIR; bruyante, données hétérogènes, avec masquages, éclairage inconsistant, flous, iris décalés
UBIRIS	800 x 600, 1 877 images	Images couleur acquises dans les longueurs d'ondes visibles; deux sessions distinctes, les images sont majoritairement de face
Multimodal Biometric Grand Challenge (MBGC)	2 048 x 2 048, 148 vidéos, durées de 1 seconde	NIR; distance focale du IOM est de 2 à 3 pieds, les images acquises lorsque les sujets marchent en direction de la camera, majoritairement des prises de face, les sujets reçoivent la consigne de regarder la caméra de balayage des iris
IUPUI multi-wavelength	1 280 x 1 024, 352 vidéos	NIR; image des 2 yeux prise à 2 moments distincts, la durée entre chaque acquisition de données est d'au moins une semaine; utilise uniquement les ondes vertes pour les essais
IUPUI Remote	1 280 x 1 024, 731 vidéos, 30 fps	NIR; le rayon d'iris moyen était de 95 pixels, les données ont été acquises en deux sessions, au moins une semaine entre chaque session, six (6) vidéos par iris, variété de position et de situations

Évaluation de la reconnaissance de l'iris par le biais d'ensembles de données sur les iris variable-qualité : résultats et analyse

Les facteurs utilisés pour l'évaluation du rendement étaient la qualité, le taux de faux rejets (TFR), le taux d'acceptation erronée (TAE) et le taux d'échec de traitement (FTPR). Les résultats sont illustrés dans les tableaux ci-dessous :

Dataset-Based Iris Recognition Accuracy

Failure to Process Rates
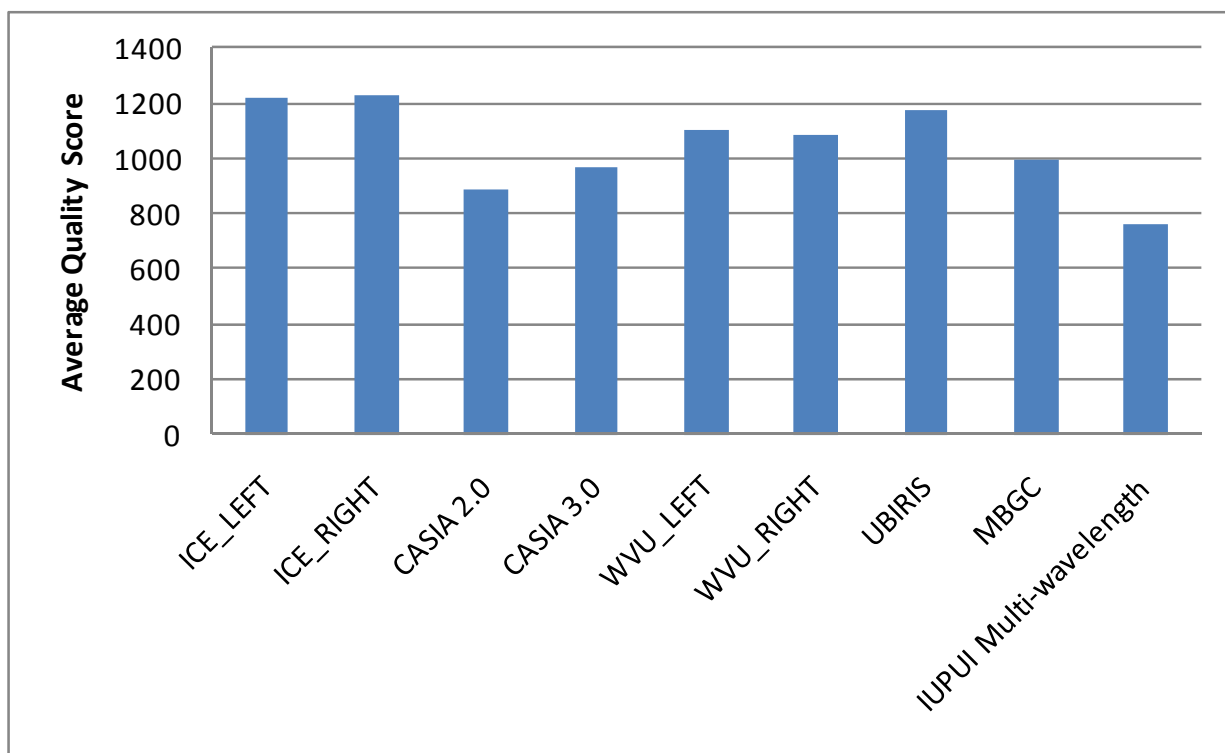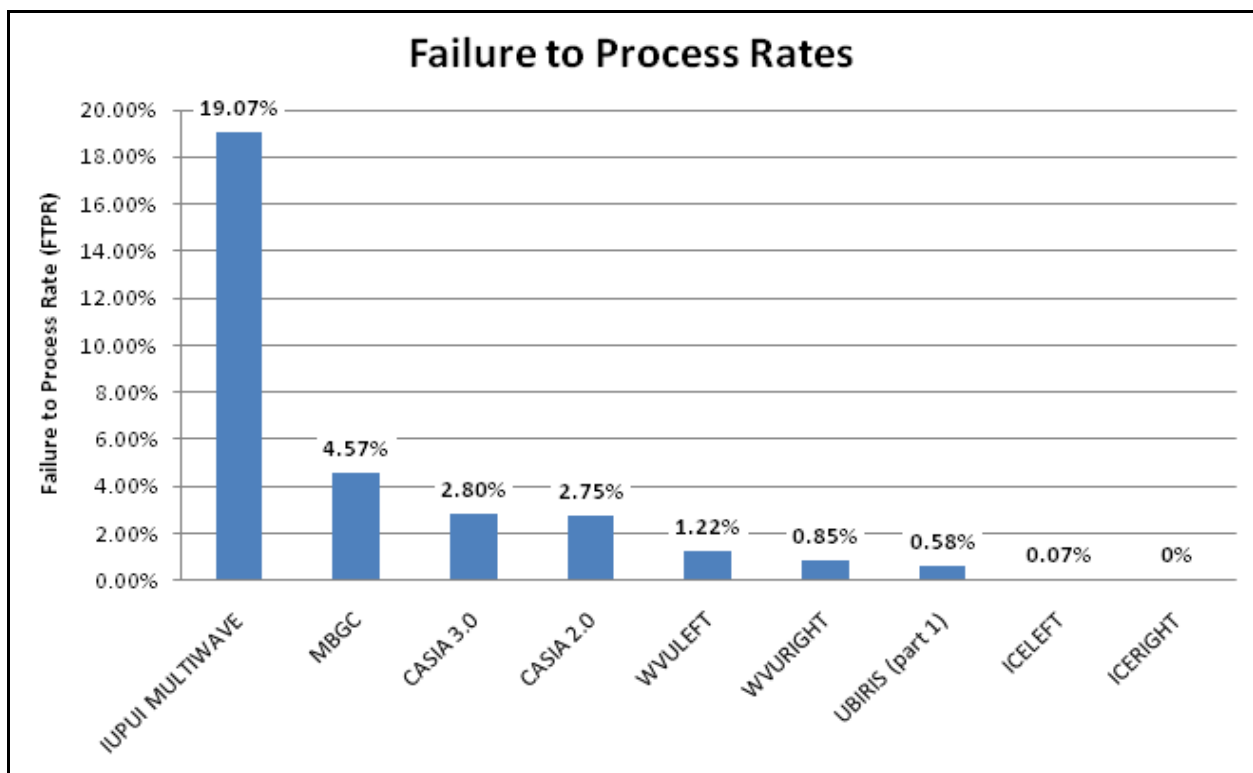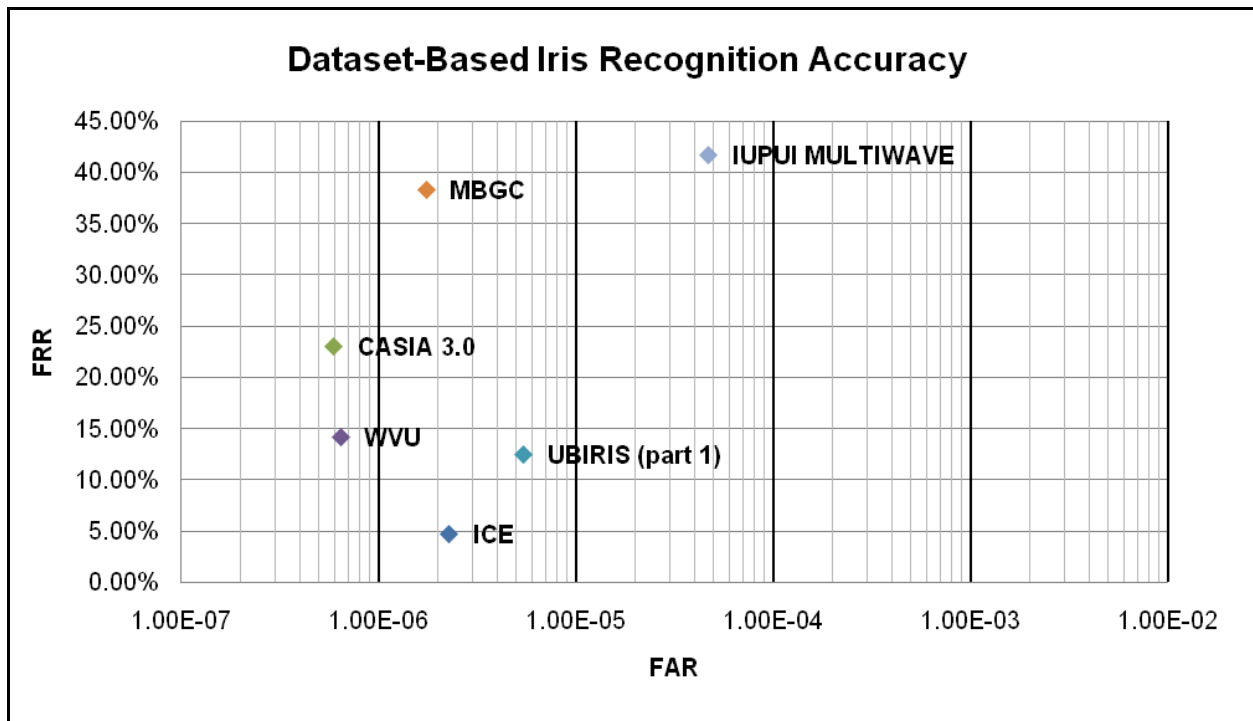
Les conclusions suivantes peuvent être tirées de cette évaluation d'ensembles de données multiples :

- Le traitement et la correspondance sont très rapides. Le système peut effectuer une reconnaissance de l'iris en 17,8 ms (y compris la segmentation, l'extraction de caractéristiques et la correspondance 1:1).
- Il possède un faible taux d'échec d'acquisition (FAR) lorsqu'on utilise un seuil de décision (distance de Hamming) de 0,33. La distance de Hamming utilisée pour l'identification à grande échelle aurait eu comme résultat un taux d'échec d'acquisition (FAR) de 0,00 % et un taux de faux rejets (TFR) plus élevés pour tous les ensembles de données.
- Le système est en mesure de traiter des images dans les longueurs d'ondes visibles, à condition que les formes d'iris soient bonnes pour la reconnaissance.
- Le système fonctionne raisonnablement bien lorsque les pupilles sont normalement dilatées.

Les points à améliorer sont les suivants :

- Le système est incapable de traiter des images non coopératives et décalées.
- Puisque le système commercialisé est conçu pour des images recueillies à l'aide d'un système d'acquisition précis et jumelé, il existe des préférences en matière de résolution de l'image et d'éclairage. En général, le système commercialisé fonctionne mieux avec des images d'iris d'une résolution d'environ 200 pixels sur tout l'iris. Cependant, le système sera en mesure d'effectuer une reconnaissance de l'iris précise si la résolution de l'image peut être adaptée adéquatement sans déformer l'iris.
- L'éclairage, le contraste et le fou animé ont une grande incidence sur la précision de la reconnaissance.
- Le système commercialisé ne peut pas fonctionner avec des images d'iris foncés dans les longueurs d'ondes visibles en raison du manque d'iris reconnaissables.
- Les distances de Hamming ne sont pas nécessairement symétriques. Lorsqu'elles sont utilisées pour l'enregistrement, les images de faible qualité ont obtenu de plus grandes distances de Hamming (moins bonnes).

Incidence de la compression sur la reconnaissance de l'iris

La compression des données commence à jouer un rôle dans l'utilisation des systèmes de reconnaissance de l'iris. Sur le terrain, les applications qui utilisent des dispositifs de reconnaissance de l'iris portatifs utilisent souvent des communications sans fil pour se brancher au serveur central lors de l'identification et de la vérification. Bien qu'il soit idéal d'avoir une bande passante large pour la transmission des applications en temps réel, il faut souvent transmettre des images saisies ou des gabarits sur un canal de communication à bande passante étroite. Dans ce cas, il faut minimiser la quantité de données à transmettre (ce qui est possible grâce à la compression) afin de diminuer le temps nécessaire pour les transmissions et d'économiser de l'énergie. L'étude a analysé des évaluations menées antérieurement sur les techniques de compression, y compris la compression des régions d'intérêt.

Reconnaissance de l'iris avec des verres de contact

Les verres de contact imprimés peuvent causer des erreurs dans le système de reconnaissance de l'iris. Les experts ont étudié l'effet des verres de contact transparents sur la précision de la reconnaissance de plusieurs systèmes. Leurs données ont été prises dans le même studio avec un éclairage ambiant intérieur constant. Les experts ont inspecté visuellement toutes les images et rejeté toutes celles de faible qualité. Ils ont ensuite classé les sujets portant des verres de contact en cinq (5) catégories distinctes. Douze mille trois (12 003) images d'iris provenant de 87 sujets portant des verres de contact et 9 697 images de sujets ne portant pas de verres de contact ont été traitées par trois (3) algorithmes de correspondance. Les sujets portant des verres de contact ont été regroupés en cinq (5) catégories différentes selon une inspection visuelle.

Catégorie 0	Aucun verre de contact
Catégorie 1	Aucune modification ou modification minime de l'iris. Tout au plus, ces images présentent un bord à peine visible.
Catégorie 2	Les images présentent une limite circulaire définie sur la zone de l'iris.
Catégorie 3	Les images présentent des verres munis d'inscriptions, des verres qui s'ajustent mal et ne sont pas à plat sur l'iris ou des verres qui produisent un artéfact.
Catégorie 4	Les images d'iris où les sujets portent des verres de contact durs. Les verres de contact durs produisent un cercle très distinct et déforment la zone qu'ils recouvrent.

Les résultats ci-dessous illustrent de légères augmentations du taux de faux rejets (TFR) dans les catégories 0 à 3, et des augmentations importantes du TFR dans la catégorie 4.
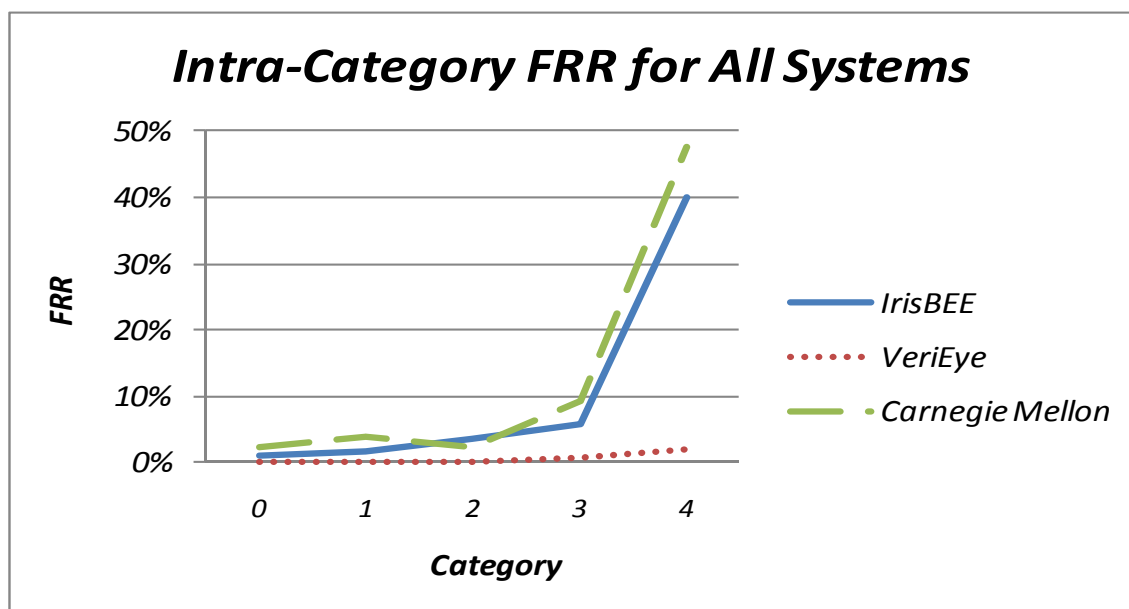
Reconnaissance de l'iris non-coopérative basée sur une vidéo

Au fur et à mesure que les technologies de reconnaissance de l'iris évoluent, elles seront en mesure d'acquérir une image sans que l'utilisateur final ne s'en rende compte. Cela fera de la reconnaissance de l'iris une excellente technique de vérification puisqu'il n'y aura pas de demande d'effort supplémentaire pour l'utilisateur. Cette technologie constitue également un bon outil potentiel pour la recherche de personnes d'intérêt puisqu'un système de reconnaissance de l'iris non-coopératif permet d'identifier des personnes sans que celles-ci ne soient mises au courant. Cette application est tout particulièrement intéressante pour la sécurité dans les aéroports, aux frontières et dans tout autre place publique.

Reconnaissance de l'iris basée sur les longueurs d'ondes multiples

Les images NIR jouent depuis longtemps un rôle prédominant dans l'identification de l'iris. L'un des désavantages de la lumière NIR est qu'elle nécessite un éclairage NIR actif. La reconnaissance de l'iris basée sur les longueurs d'ondes visibles pourrait fonctionner à l'aide d'un éclairage environnemental. De plus, la reconnaissance basée sur les longueurs d'ondes visibles est importante, car elle peut être utilisée de concert avec la reconnaissance faciale pour les données biométriques multimodales. Dans quelques années, les caméras de surveillance en couleur normales pourraient être en mesure d'effectuer la reconnaissance de l'iris. La reconnaissance de l'iris basée sur les longueurs d'ondes visibles présente

ses défis, notamment pour les yeux de couleur foncée et pour la reconnaissance à distance. On pourrait voir apparaître dans l'avenir un système de reconnaissance de l'iris à longueurs d'ondes multiples, lequel pourrait être utilisé de concert avec un système de reconnaissance faciale à longueurs d'ondes multiples pour la surveillance vidéo.

Reconnaissance multimodale des yeux

Les motifs complexes et détaillés des yeux de couleur foncée ne peuvent être révélés que sous une lumière NIR et c'est pourquoi une image d'iris obtenue à longue distance est beaucoup moins précise. Si on obtient une image d'iris à l'aide d'une lumière visible, les motifs de l'iris des yeux de couleur foncée seront pratiquement invisibles. La sclérotique, la couche protectrice extérieure blanche et opaque de l'œil, peut également être utilisée pour identifier les humains. Le processus de segmentation de l'image de la sclérotique comprend le sous-échantillonnage de l'image, la conversion de l'espace couleur HSV, l'estimation de la région de la sclérotique, la détection de l'iris et de la paupière, le raffinage des limites de la paupière et de l'iris, la création d'un masque et le suréchantillonnage du masque. La région de la sclérotique est estimée à l'aide de la meilleure représentation entre deux techniques fondées sur les couleurs.

Évaluation du rendement des technologies ACDB basées sur les empreintes digitales GenKey

Technologie GenKey

GenKey, un important fournisseur de solutions pour l'amélioration de la confidentialité des données biométriques, a développé un algorithme biocryptique qui fait le pont entre la cryptologie et les données biométriques. Cet algorithme breveté convertit une image biométrique en clés cryptographiques compatibles avec l'infrastructure à clés publiques (ICP) qui sont irréversibles et ne partagent aucune relation mathématique avec les sources biométriques qu'elles représentent. Ses solutions peuvent être appliquées à une variété de contextes, y compris l'éducation, l'homologation et les soins de santé. L'algorithme GenKey offre un moyen d'enregistrer et de contrôler des individus en se basant sur les renseignements biométriques comme les empreintes digitales. L'algorithme offre diverses options entre la vitesse de reconnaissance, la précision et la confidentialité des données biométriques.

Gabarit de caractéristiques GenKey par rapport aux enregistrements de clé d'identification

L'algorithme GenKey peut effectuer deux types d'enregistrement. Dans le cas de l'enregistrement du gabarit de caractéristiques, les caractéristiques discriminantes des images d'empreintes digitales sont extraites et stockées dans un gabarit de données biométriques pour un individu donné. Le gabarit des caractéristiques est stocké pour usage ultérieur et l'image biométrique peut être supprimée. L'enregistrement de clé d'identification permet aussi d'extraire des caractéristiques discriminantes des images d'empreintes digitales, mais il convertit les caractéristiques en une valeur numérique qui représente les données biométriques de l'individu. À la fin de l'enregistrement d'une clé d'identification, la clé (valeur numérique) est stockée et l'image biométrique et le gabarit de caractéristiques peuvent être supprimés. Ce type d'enregistrement est le centre d'intérêt de l'évaluation du rendement d'IBG.

IBG a mis à l'essai deux types de clé d'identification GenKey :

- Les **clés d'identification standard** offrent un rendement semblable au rendement des enregistrements du gabarit de caractéristiques.
- Le désavantage des **clés d'identification flexibles** est la taille et la précision des clés.

IBG a évalué le rendement des clés d'identification standard, de même que celui des clés d'indentification flexibles de 12, 25, 56 et 107 octets.

	Gabarit de caractéristiques (pas une technologie ACDB)	Clé d'identification standard (technologie ACDB)	Clé d'identification flexible (technologie ACDB)
Précision	Les enregistrements des caractéristiques offrent le rendement le plus fiable.	Les clés d'identification standard fonctionnent avec des taux d'erreurs peu élevés comparativement aux gabarits de caractéristiques.	Les clés d'identification flexibles offrent une variété d'options de précision en matière de rendement. Les clés plus grosses offrent une précision semblable aux clés standard.
Confidentialité	Offre une certaine confidentialité pour les empreintes digitales; l'accès à un gabarit de caractéristiques ne donne pas à un utilisateur malveillant la capacité de reconstruire l'empreinte digitale originale. Avec une connaissance du processus de création du gabarit de caractéristiques GenKey, un utilisateur malveillant pourrait accéder aux renseignements généraux relatifs à la structure de l'empreinte.	Les clés d'identification offrent un avantage de confidentialité par rapport à l'enregistrement de gabarits de caractéristiques. Un utilisateur malveillant ayant accès à une clé d'identification ne peut pratiquement pas régénérer les caractéristiques des empreintes digitales ou extraire des renseignements détaillés relatifs à la structure de l'empreinte. La technique utilisée pour convertir le gabarit de caractéristiques en une clé est semblable à une fonction cryptographique unidirectionnelle. Il est facile de calculer une clé d'identification à partir d'un gabarit de caractéristiques, cependant il est impossible, sur le plan des calculs, de renverser le processus.	
Débit de traitement	Les enregistrements de caractéristiques permettent les recherches les plus rapides. L'algorithme GenKey est en mesure d'effectuer des millions de correspondances du gabarit de caractéristiques par seconde à l'aide de matériel informatique normal.	Bien que pas aussi efficace que la correspondance des gabarits de caractéristiques, la vérification des clés d'identification peut aussi être effectuée assez rapidement à l'aide de matériel informatique ordinaire. GenKey procède à l'estimation de centaines de milliers de vérifications par seconde. La vitesse de correspondance augmente (c.-à-d. un ralentissement) au fur et à mesure que des seuls de correspondances plus strictes sont appliqués.	
Taille type de la clé	128-256 octets	64-128 octets	12-107 octets

Données d'essai du GenKey

IBG a utilisé une banque d'environ 6 000 images d'empreintes digitales plates (index gauche et droit)

provenant de 1 200 sujets, lesquelles ont été recueillies à l'intérieur. Les images des empreintes digitales ont été recueillies à l'aide d'un *Cross Match Verifier* de 500 ppp. Chaque sujet a donné deux échantillons par doigt lors de la première visite. Par ailleurs, environ 650 des 1 200 sujets ont offert deux échantillons par doigt lors de leur deuxième visite, laquelle a eu lieu environ un mois après la première.

Processus d'enregistrement et de reconnaissance GenKey

À l'aide d'une trousse de développement de logiciel (SDK) fournie par GenKey, IBG a développé une application personnalisée qui a permis d'extraire les caractéristiques, de créer un gabarit et de créer une clé d'identification. Les deux empreintes de l'index devaient s'être enregistrées afin que la saisie soit considérée un succès. IBG a aussi développé une application personnalisée qui effectuait la correspondance en bloc. Les images d'empreintes digitales obtenues lors de la deuxième visite ont été utilisées pour la reconnaissance (p. ex. : comme images de sondage) et ont été comparées aux données de la première visite.

En plus d'utiliser l'algorithme GenKey pour traiter les données, IBG a procédé au traitement des mêmes ensembles de données d'empreintes digitales avec un algorithme largement adopté basé sur les empreintes et points caractéristiques *Neuortechnology VeriFinger*, version 6.3. L'approche de traitement *VeriFinger* était équivalente à l'approche GenKey décrite ci-dessous. La comparaison et le contraste des résultats GenKey et des résultats *VeriFinger* permettent d'obtenir un cadre général de référence pour valider la viabilité commerciale de la technologie des clés d'identification GenKey.
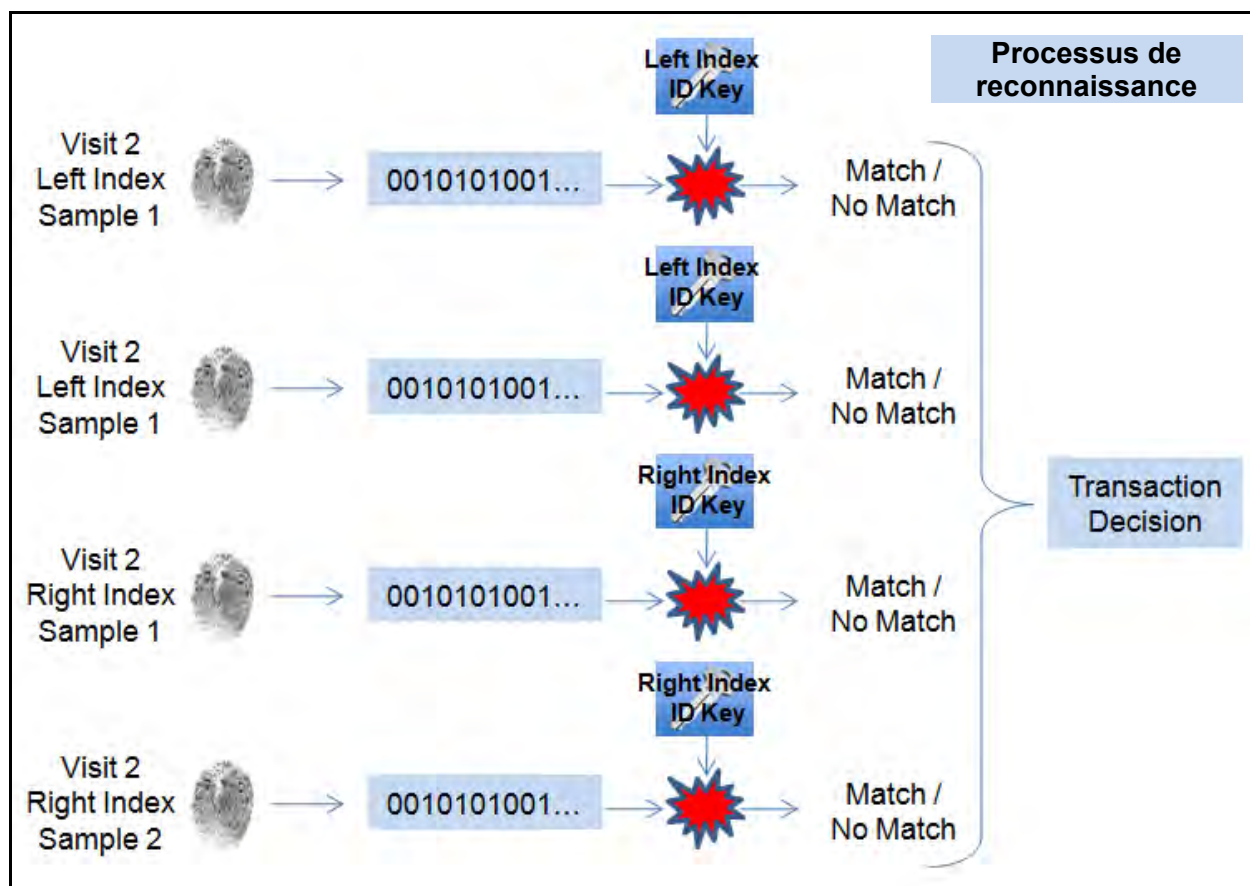
Les volumes de traitement sont illustrés ci-dessous.

	GenKey	VeriFinger 6.N
Sujets	650	650
Comparaisons acceptables	456	459
Comparaisons imposteurs	550 976	560 741

Résultats des essais GenKey

En se fondant sur les processus de collecte et de comparaison décrits ci-dessus, les mesures suivantes ont été obtenues :

Mesures de convivialité	Mesures de précision
• Taux d'échec d'encodage (FTE) • Taux d'échec d'acquisition (FTA) • Temps de traitement	• Taux de fausse correspondance (FMR) • Taux de fausse non-correspondance (FNMR) • Distribution des erreurs par sujets

Échec de l'enregistrement	Tentatives d'enregistrement	Compte FTE	Taux FTE
VeriFinger 6.3	2 448	42	1,72 %
Clé d'identification	2 448	45	1,84 %

GenKey			

Échec d'acquisition	Tentatives d'encodage de reconnaissance	Compte FTA	Taux FTA
VeriFinger 6.3	1 841	1	0,05 %
Clé d'identification GenKey	1 841	66	3,59 %

Les résultats démontrent que les taux d'échec d'encodage (FTE) de GenKey et de *Verifinger* sont pratiquement équivalents, tandis que le taux d'échec d'acquisition (FTA) de GenKey est de beaucoup supérieur à celui de *VeriFinger*. Cela permet de mettre en évidence le concept que GenKey utilise des images de haute qualité, lesquelles sont validées en temps réel au point de saisie.
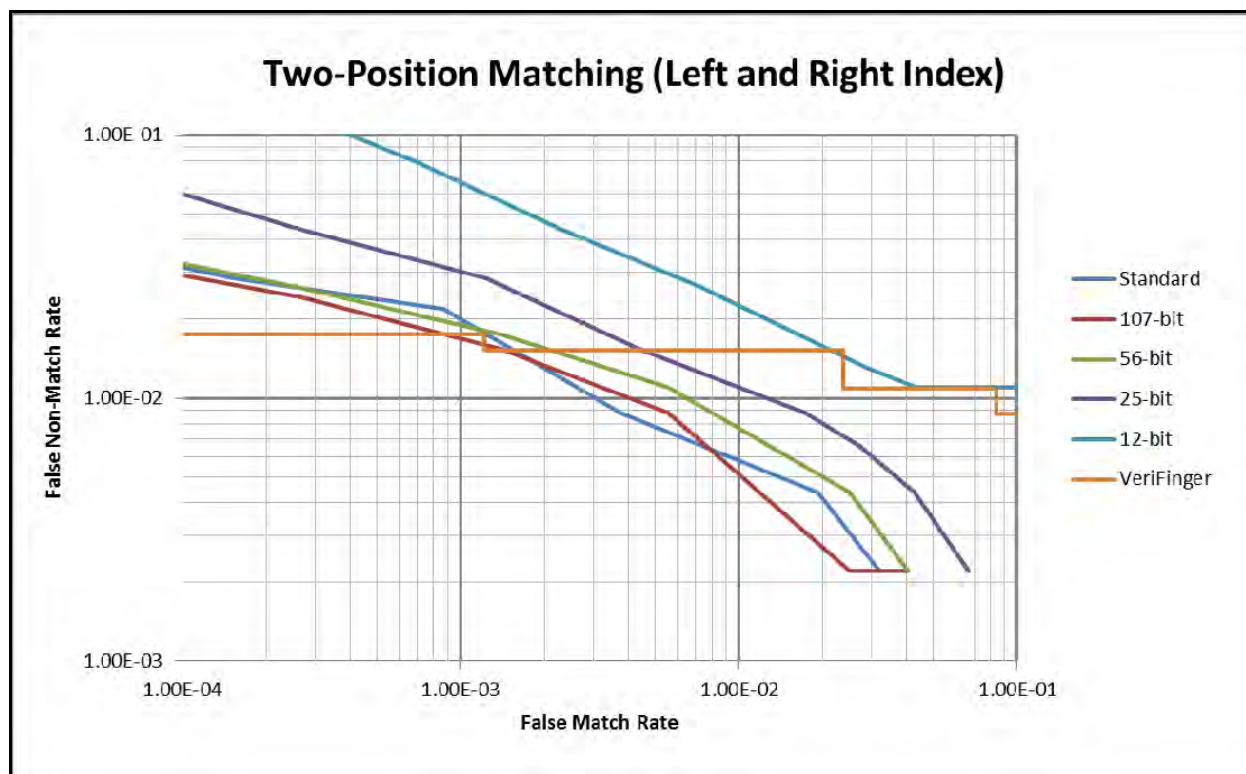
Une évaluation du rendement comparative avec un ensemble de données difficiles démontre la viabilité des technologies ACDB commerciales utilisant les empreintes digitales. Le rendement des technologies ACDB est très semblable de celui d'un coupleur fondé sur les points caractéristiques mis à l'essai par NIST et largement déployé.

Pour de nombreux systèmes biométriques, certains sujets obtiennent des taux de fausses correspondances plus élevés que d'autres. IBG a analysé la distribution de fausses correspondances chez les sujets. Les taux de fausses correspondances spécifiques aux sujets (cumulés à partir de tous les types et de toutes les tailles de clé d'identification et mesurés à un seuil type de 0,45) se situaient aussi haut que 4,04 % et aussi bas que 0,00 %. Bien que les taux de fausses correspondances décroissent généralement lorsque la taille des clés augmente, dans certains cas les sujets ont connu des taux de fausses correspondances plus élevés avec de plus grosses clés. Par exemple, 251 des 457 sujets ont connu des taux de fausse correspondance plus élevés avec des clés d'identification de 56 octets qu'avec des clés de 25 octets.

Conclusions

Les conclusions suivantes peuvent être tirées de la présente étude :

- Les aspects du rendement de la reconnaissance non-coopérative de l'iris, y compris le taux élevé d'enregistrement et de fausses non-correspondances, compliquent son utilisation comme technologie ACDB.
- La saisie de reconnaissance de l'iris contrôlée ou les images d'iris de haute qualité accroîtront l'usage de l'iris comme technologie ACDB.
- Une évaluation du rendement comparative et un ensemble de données difficiles démontrent la viabilité des technologies ACDB commerciales utilisant les empreintes digitales.
- Le rendement de GenKey est très semblable à celui d'un coupleur fondé sur les points caractéristiques mis à l'essai par NIST et largement déployé.
- Les personnes chargées de la mise en œuvre devraient étudier comment incorporer les approches fondées sur les clés à l'architecture de leurs applications.

1   Background and Objectives

This document is the Study Report for PSTP 02-0351BIO, **Biometric Data Safeguarding Technologies Analysis and Best Practices**.

Biometrics is one of two approved Communities of Practice (CoPs) under Public Security Technical Program's (PSTP's) Surveillance, Intelligence, and Interdiction (SII) Domain. SII encompasses capabilities that allow Canada to monitor the security environment, understand the threats to national security, and direct an effective and proportionate response to deter, disrupt, or defeat threats to Canada. Biometrics can assist these efforts by using technology to capture biometric samples, perform feature extraction or dataset creation, and perform one-to-one or one-to-many searches to identify or confirm the identity of individuals.[1]

One of the main goals of PSTP's Biometrics CoP is to evaluate, analyze, and implement biometric technologies that enhance national capabilities in access control, identity verification, and e-Commerce security in a manner that is consistent with Canadian laws and acts. This is done in collaboration with the appropriate Government of Canada agencies and departments responsible for national security, border control and security, and law enforcement and immigration. This effort will also be leveraged through the Memorandum of Understanding (MOU) that establishes collaborative science and technology (S&T) with the United States Department of Homeland Security.

The rapid progress of biometrics technology in the last few years and the ease with which biometrics data can be acquired has resulted in the accumulation of large varying databases of biometrics information. This trend will continue in the future, with databases growing at an ever-increasing rate. The purpose of the Study is to examine some of the issues surrounding the sharing and safeguarding of biometric data in the Canadian Public Security context writ large. Throughout the study, the modality focus will be on iris biometrics (prime focus) and fingerprints (secondary).

The primary objective of this work is to support the Biometrics CoP by leading scientific studies that identify and evaluate biometric technologies with respect to their ability to be used securely (in terms of safeguarding biometric databases). These new biometric technologies and associated data safeguarding capabilities must be consistent with the Government of Canada's dual prosperity and security mandates, and must consider legal, ethical, cultural, and privacy issues.

Biometric privacy enhancing technologies (PETs) are among the most promising technologies for data safeguarding. These technologies leverage biometric information to improve and ensure personal privacy while protecting sensitive information and assets. PETs can be categorized as follows:

- **Untraceable Biometrics** – defined by Dr. Ann Cavoukian, Ontario Privacy Commissioner, as a new class of emerging privacy enhancing technologies such as biometric encryption
- **Anonymous Biometrics** – a system where biometric data are not connected to any personal data; biometric data can be taken to another system to connect with personal information
- **Revocable ("Private") Biometrics** – allow people to have multiple biometric identities using the same biometric information; identities can be used independently or anonymously

Study PSTP 02-0351BIO addresses Biometric Data Safeguarding Technologies Analysis and Best Practices through the following tasks.

- Review the emergence of biometrics for defence and security and identify the issues surrounding data sharing and safeguarding
- Compare and contrast biometric technologies for biometric data safeguarding that are currently in use or planned for use in other national and international jurisdictions
- Evaluate the applicability of these biometric technologies and associated data safeguarding constraints in terms

---

[1] http://www.css.drdc-rddc.gc.ca/pstp/proj-prop/call-appel/biometrics-biometrie/biometrics-biometries00-eng.asp

of supporting cross-jurisdictional public security environments
- Evaluate state-of-the-art biometric technologies and their vulnerabilities in terms of protecting identity and complying with federal privacy standards and policies
- Survey and evaluate associated issues of interoperability, database sharing, and format sharing internationally and interdepartmentally, and identify any emerging biometric technologies (e.g., multilevel security solutions) that may offer potential solutions
- Address issues of cost, Canadian privacy policy, and Technology Readiness Level (TRL) of these data safeguarding technologies or procedures, with timeframe projections for implementation

The Lead Federal Department for the Study is Canada Border Services Agency (CBSA). Addition partners include the following:

- Royal Canadian Mounted Police
- Transport Canada
- Defence Research and Development Canada (DRDC) – Toronto
- Office of the Information and Privacy Commissioner of Ontario
- University of Toronto
- Indiana University-Purdue University Indianapolis (IUPUI)
- IBG-Canada (Study Report author)

2 Biometric Data Safeguarding in Defence and Security Applications

Emergence of biometric technology in defence and security applications has resulted in the creation of large-scale datasets of biometric information of both national and international scale and presenting a new set of challenges regarding privacy and data safeguarding of personally identifiable datasets. Biometric datasets represent very sensitive personally identifiable information. When used to authenticate a subject's transactions, they could be misused to track the subject's actions and movements. In the case of fingerprints, biometric datasets could even be used to falsely incriminate the subject in a physical crime. This section examines the types of biometric technology prevailing in defence and security applications and identifies potential threats to security and privacy surrounding data sharing and safeguarding in biometric-enabled applications.

2.1 Biometric Technologies: Operation, Strengths, and Weaknesses

Leading biometric technologies for defence and security scenarios include fingerprint recognition, face recognition, and iris recognition. The basic operations, strengths, and weaknesses of each technology are discussed below.

2.1.1 Fingerprint

Fingerprint technology utilizes the distinctive features to identify or verify the identity of individuals. Fingerprint recognition is the most commonly deployed biometric technology, used in a broad range of physical and logical access applications. Fingerprint recognition refers to use in either 1:1 verification or small-scale identification against hundreds or thousands of enrolled records. Large-scale systems that match millions of fingerprints are referred to as AFIS (automated fingerprint identification systems). AFIS implementations are much more complex than 1:1 fingerprint implementations, though defence and security applications often deploy both 1:1 and 1:N systems.

Fingerprint systems are comprised of image acquisition hardware, image processing components, template generation and matching components, and storage components. These components can be located within a single peripheral or standalone device, or may be spread between a peripheral device, a local PC, and a central server. High-level strengths and weaknesses are shown in Figure 1.

Fingerprint: Strengths	Fingerprint: Weaknesses
- Proven technology capable of high accuracy - Performance (accuracy, throughput) of leading technologies is well-documented and understood - Ability to enroll multiple fingers; exceptionally high accuracy for ten print collections - Ergonomic, easy-to-use devices - Fingerprint data is almost universally interoperable, facilitating searches against watchlists	- Performance can deteriorate over time - Association with forensic applications - Users can intentionally damage fingerprints, reducing performance - Implementation of large-scale systems requires highly specialized expertise for performance tuning and optimization

Figure 1: Fingerprint Strengths and Weaknesses

The five stages involved in fingerprint verification and identification are image acquisition, image processing, location and encoding of distinctive characteristics, template creation, and template matching.

Fingerprint systems acquire one or more fingerprint images and convert images to digital format. Image processing subroutines eliminate gray areas from the image by converting the fingerprint image's gray pixels to white and normalizing ridge width and flow. Fingerprint recognition systems utilize proprietary algorithms to map the absolute and relative position of minutiae, the distinctive points found in fingerprint ridges. Large-scale systems also use ridge flow information. Algorithms compare template data from one or more fingerprints, working through permutations of minutiae offsets to identify and score similarities. The resulting acceptance or rejection of the user's access is based on reaching an acceptable level of correlation between the two templates. A correlation threshold is necessary because subtle changes in fingerprint placement and minutiae recognition mean that no two fingerprint templates will be exactly alike.

Positive and negative error rates, as well as enrollment failure rates, are low for most fingerprint devices and systems, assuming that multiple fingerprints are acquired on enrollment. A small percentage of users, varying by the specific technology and user population, are unable to enroll in some fingerprint systems. Furthermore, certain demographic groups – such as elderly populations and manual laborers – often have lower quality fingerprints and are more difficult to enroll. Although the fingerprint is a stable physiological characteristic, a variety of factors can cause the performance of some fingerprint recognition technologies to worsen drastically over time, particularly when a limited number of fingerprints are used for matching. Although high-quality enrollment improves long-term performance, users who work with their hands are likely to see increased error rates over time.

Fingerprint recognition technology includes peripheral devices, imbedded devices, wall mounted devices, and large units designed for heavy-duty operation. For border control deployments, the primary question in terms of device selection is whether to deploy single-finger readers or ten-print devices (see Figure 2). US-VISIT was initially deployed with single-finger readers, and migrated to ten-print devices when it became clear that more than two fingerprint positions would be necessary to maintain acceptable levels of accuracy and match speed for that deployment's immense transaction volume. Single-finger readers are suited for deployments in which no more than two positions (e.g. left and right index) are acquired. Increasingly, agencies are making the investment in ten-print devices capable of acquiring all ten finger positions in three placements (left 4, right 4, and thumbs). The collection of ten prints not only reduces collection errors (e.g. swapping left for right), but it increases the scalability, accuracy, and speed of fingerprint matching by orders of magnitude relative to 1- or 2-position systems.

Figure 2: Single-Finger and Ten-print Devices

Large-scale defence and security applications deploy AFIS technology in their identification systems around the world as the technology is a proven, central, and established part of law enforcement and security check processes. Although biometrics cannot solve the problem of fraudulent identity documents being used to establish an identity, they can address the problem of duplicate identities creation. Such systems will provide both AFIS and 1:1 functionality.

2.1.2 Face Recognition

Face recognition technology utilizes distinctive facial features to verify or identify individuals. Face recognition is primarily deployed in 1:N applications, though improvements in system and workflow design (as well as digital imaging) have increased the performance of face recognition in 1:1 applications. Used in conjunction with ID card systems, booking stations, and for various types of surveillance operations, face recognition's most successful implementations take place in environments where cameras and imaging systems are already present.

Face recognition systems can range from software-only solutions that process images acquired through existing cameras (e.g. still or CCTV) to full-fledged acquisition and processing systems with dedicated cameras and illuminators. In some face systems, the core technology is optimized to work with specific cameras and acquisition devices. More often, the core technology is designed to enroll, verify, and identify face images acquired through various methods such as static photographs, web cameras and surveillance cameras. Face recognition systems are not often integrated into 1:1 physical access applications and are more likely to be used in large-scale identification or surveillance. High-level strengths and weaknesses are shown in Figure 3.

Face Recognition: Strengths	Face Recognition: Weaknesses
• Does not require user training or effort • Can often leverage existing image datasets and existing photograph processes	• Susceptible to high false non-match rates in 1:1 and 1:N applications • Changes in acquisition environment reduce matching

• Capable of identification at a distance • Capable of rapid 1:N identification with relatively little processing power • Performance improves hand-in-hand with camera quality and image resolution	accuracy • Changes in physiological characteristics reduce matching accuracy • Lighting, camera angle reduce matching accuracy

Figure 3: Face Recognition Strengths and Weaknesses

Face recognition technology is based on the standard biometric sequence of image acquisition, image processing, distinctive characteristic location, template creation, and matching. Face recognition technology can acquire faces from almost any static camera or video system that generates images of sufficient quality and resolution. Ideally, images acquired for face recognition will be acquired through high-resolution cameras, with users directly facing the camera, and with moderate lighting of the face.

Face images are normalized to overcome variations in orientation and distance. In order to do this, basic characteristics such as the middle of the eyes are located and used as a frame of reference. Once the eyes are located, the face image can be rotated clockwise or counter-clockwise to straighten the image along a horizontal axis. The face can then be magnified, if necessary, so that the face image occupies a minimum pixel space. Once an image is standardized according to the vendor's requirements, the core processes of distinctive characteristic location can occur. Features most often utilized in face recognition systems are those least likely to change significantly over time: upper ridges of the eye sockets, areas around the cheekbones, sides of the mouth, nose shape, and the position of major features relative to each other. Face recognition is not as effective as fingerprint or iris recognition in identifying a single individual from a large dataset. A number of potential matches are generally returned after large-scale face recognition identification searches. For example, a system may be configured to return the 10 or 100 most likely matches on a search of a 1m-person dataset. A human operator would then determine whether any candidates are legitimate matches.

Relative to fingerprint and iris recognition, face recognition systems encounter higher false non-match rates over time, as the effects of aging seem to impact face recognition performance to a greater degree than fingerprint or iris recognition. The performance gap narrows if very high-resolution face images are used for enrollment and matching. Assuming that face images are acquired from a fixed distance under consistent lighting and background conditions, the technology is substantially more accurate than is perceived. Simple changes in user appearance can to have an impact on systems' ability to reliably identify enrolled users. Changes in hairstyle, makeup, or facial hair, or addition or removal of eyeglasses, can cause users to be falsely rejected. Emerging techniques, such as 3D reconstruction and modeling, have led to the development of more robust algorithms which may be less susceptible to such changes.

In an effort to reduce environmental impact on accuracy, deployers and practitioners have become much more cognizant of the role of image quality in face recognition accuracy. When face recognition systems perform poorly (e.g. encounter high false non-match rates), the culprit is often the imaging process as opposed to the matching algorithm. Deployers now, whenever possible, integrate real-time face image quality validation at the point of capture. By enforcing the quality of input images, the overall accuracy and scalability of face recognition systems improves substantially. This approach also brings face recognition system design closer to that of fingerprint and iris systems, both of which implement rigorous control on input image quality.

2.1.3 Iris Recognition

Iris recognition technology encodes and matches iris patterns to identify enrolled users. Iris recognition systems are comprised of collection devices and encoding / matching engines. Collection devices (see Figure 4) include advanced imaging and optics components along with one or more infrared illuminators. Images may be encoded and matched on the device, on a host PC, or on a central server.

Figure 4: Iris Recognition Form Factors[2]

Iris recognition technology requires the acquisition of a high-resolution, infrared-illuminated image to effectively locate and encode iris data. Iris recognition technology is imbedded in peripheral cameras no larger than typical web cams, and is also build into wall-mounted and kiosk-based form factors for access control and identification applications. The latter types have been deployed successfully in air travel applications, and are generally capable of acquiring higher-quality iris images (and therefore providing higher degrees of accuracy).

Once the iris is located and segmented, a grayscale image is used for feature extraction. Characteristics derived from the iris include the orientation and spatial frequency of furrows and striations. Iris recognition is recognized for (1) resistance to false matching regardless of dataset size and (2) rapid searches of large datasets. Assuming that thresholds are properly implemented, false positive matches should be exceptionally rare. In fact, some iris systems are implemented such that all matches are assumed to be positive. The tradeoff is that iris systems may be more prone to false negatives (in which an enrolled subject is falsely not identified) than, for example, fingerprint systems. High-level strengths and weaknesses are shown in Figure 5.

Iris Recognition: Strengths	Iris Recognition: Weaknesses
• Exceptionally resistant to false matching • Default operation is identification mode • High stability of characteristic over lifetime • Hands-free operation • Real-time searches against large datasets (e.g. 10m irises) are possible with modest CPU loads	• Acquisition of iris image requires more training and attentiveness than most biometrics • User discomfort with eye-based technology • Glasses can impact performance • Propensity for false non-matching or failure to capture

Figure 5: Iris Recognition Strengths and Weaknesses

The acquisition process, and the effort required on the part of the user, differs from device type to device type. More so than in many biometric systems, users must be cognizant of the manner in which they interact with the system: iris acquisition requires fairly precise positioning of the head and eyes. Several types of devices are used in iris recognition applications, some of which are better suited to usage in border applications than others. Regardless of the acquisition device, individuals are required to position themselves at a specified distance from the camera; distances range from a few inches to a few feet. Certain devices may prompt the user with verbal instructions.

---

2 http://www.aoptix.com/biometrics/AOptixBiometrics-DS6P.pdf

The iris recognition market has undergone a radical transformation since the late 2000's. Up to that point, a single vendor dominated the market for matching technology, and capture devices had to deliver images that conformed to this vendor's requirements. Since then, numerous iris recognition algorithms have become commercially available; independent testing has demonstrated that many newer algorithms are roughly on par with more established algorithms in terms of speed and accuracy. Further, numerous capture devices have come to market – ranging from low-end peripherals to high-end stand-off devices – greatly expanding the range of applications for iris recognition technology. Perhaps most importantly, current-generation iris systems collect and store iris images as opposed to proprietary templates. Therefore one of the largest impediments to iris recognition adoption in defence and security applications – that of reliance on proprietary data formats – is a non-issue in most modern iris recognition systems.

2.1.4   Multiple biometrics

Multiple biometric solutions involve the submission of more than one biometric characteristic for verification or identification. These submissions can be simultaneous or serial; a second biometric sample may be required if a primary biometric is rejected, or may be required for each verification or identification. Multiple biometric solutions can be designed to decrease FTE rates, as users unable to enroll in one biometric technology will generally be able to enroll in a second technology. This reduces the need for non-biometric fallback processing. Multiple biometrics can be used to increase security by requiring that an imposter defeat two biometrics to be verified; they can also increase convenience by allowing an individual to verify on a secondary biometric if the first biometric fails.

Using multiple biometrics also allows for the introduction of sophisticated decision logic when verifying or identifying individuals. Beyond a simple yes/no decision in which an individual must match in two systems in order to be verified, "fusion systems" can be implemented in which a near-match in one system allows a lower score in a second system to constitute a match. Similarly, a very low score in one biometric system may require a very high score in a second system in order for an individual to be declared a "match". By combining raw scores from vendor technologies, and adjusting thresholds based on application-specific requirements, deployers can implement more flexible systems. In addition, using multiple biometrics during enrollment may allow for more rapid and more accurate searches. If one technology is used as a gross classifier, such that a technology eliminates 60% of individuals in a dataset in a rapid 1:N search, then a more robust 1:N technology can be used to search the remaining 40% of individuals for duplicates.

Many large-scale civil and criminal identification systems utilized in defence and security applications process multiple biometric facets during enrollment. This results in creation of biometric profiles for large numbers of individuals that enable future functionality through different technology combinations. Multimodal biometric systems can mitigate certain performance and robustness limitations associated with single-modality systems. A multimodal biometric system based on non-correlated traits is expected to improve matching accuracy and to increase protection against spoof attacks.

Civil ID, inclusive of passport, national ID, and entitlement applications, is the strongest application for multiple biometric systems. The use of multiple biometrics in complex programs such as US VISIT and registered traveler, as well as the allowance for multiple biometric solutions in passport applications, underscore the viability of this approach. Civil ID applications are mandatory and must be capable of operating for the very large majority of potential users. In addition, civil ID applications may have a large number of enrollees, such that multiple biometric systems may be necessary to provide sufficient accuracy and response times. Civil ID applications may need to search watchlists with fingerprint, face, and even iris data, providing an additional rationale for acquiring multiple biometrics upon registration.

Access control, particularly to high-security facilities in unattended environments, is a strong environment for multiple biometric solutions. Such applications are generally unattended and must be capable of operating for an entire population. A challenge in this application is to ensure that the device can acquire data quickly enough to not impede throughput unnecessarily. Criminal ID applications have already begun to migrate to multiple biometrics systems, using face recognition in conjunction with fingerprint.

2.2   Biometric Data Sharing and Safeguarding Considerations

The scale and complexity of biometric samples gathered by national and international systems are increasing and becoming widespread. The current maturity level of biometrics has facilitated the use of biometrics in a wide range

of government applications, while much work remains in devising acceptable ways of controlling the use, storage, and exchange of biometric data and personally identifiable information. This section examines risk and threat areas associated with data sharing, and presents safeguarding techniques currently ongoing in research and deployments.

2.2.1 Privacy Threats

Privacy threats related to biometrics have been discussed extensively. Major privacy risk areas are described as followed:

- The ability to cross match data subjects across different services or applications by comparing biometric templates.
- The possibility to extract sensitive information from the stored biometric data
- The extension of application scope of biometric technology outside consent of the owner

The first threat concerns the persistence and uniqueness of biometric characteristics that allows the enrollee to be linked between different datasets. For example, an attacker could link different financial service records across different banks' datasets to one specific customer to illegally obtain the customer's financial condition or investment plan. The second threat concerns linkage between one's biometric data with other personally identifiable information, such as subject's ethnic background, health records, or visa status. Such data could in principle be abused by healthcare insurance providers; utilizing biometric templates intended for patient identification in a hospital could be used to differentiate in insurance premiums. Similar threats could occur in other application areas as well.

Other privacy risk associated with biometrics is often referred to as function creep. If the application scope of biometric technology is not well defined and restricted, its use may expand to other applications or services. For example, an application initially intended to prevent misuse of municipal services may gradually be extended to rights to buy property, to travel, or serve in armed forces. As a consequence, data subjects that would agree to use biometrics for the initial application would be forced to use biometrics for other applications.

2.2.2 Security Threats

The various security threats associated with data sharing and safeguarding can be described by potential attacks on various components of a biometric systems.

Risks during biometric data capture

The most prominent security threat during biometric data capture is enrollment of a bogus biometric characteristic. Spoofing attack is the fabrication and presentation of a fake physical biometric characteristic during enrollment and/or verification. Some biometric characteristics are harder to forge, such as the iris, while others are easier to forge, such as face or fingerprint. Since biometric information cannot be regarded as secret, the original biometric characteristic can be obtained with or without the permission or cooperation of the data subject. The sensor spoofing attack can be implemented as a coercive or impersonation attack. A coercive attack is an attack where the authorized data subject's biometric data is presented in an illegitimate scenario. An impersonation attack involves changing one's appearance so that measured biometric data matches an authorized individual. Impersonation attacks pose greater risk in regards to data security and safeguarding through tampering with the integrity of the biometric dataset with fake samples and statistics. In addition, an attacker can steal templates from a dataset and construct a synthetic biometric sample that passes authentication. Multiple biometric systems reduce the exposure to an impersonation attack through checking for consistency between different modalities.

Risks during data storage

Biometric dataset inherently poses various security threats related to its temperament. Biometric templates and data can be accessed illegally, or could be replaced or changed. In addition, biometric dataset, once compromised, biometrics cannot be updated or reissued in the same manner as passwords or ID card. The unauthorized access or modification of biometric data may not only lead to security threats, but could also extend to threats in the privacy domain, such as cross matching of different biometric datasets.

Risks during data transmission

Biometric data, scores, and decision are transferred in open and distributed systems between various agencies. Attacks can focus on changing algorithms or exchange protocols of the system by means of a Trojan horse attack. In addition, biometric dataset during data transmission is potentially vulnerable to eavesdropping, replay, brute force, and man-in-the-middle attacks[3].

2.2.3 Privacy Requirements

Safeguarding data privacy in a biometric context is a challenging task. These requirements must be followed in order to establish and deploy privacy-sympathetic biometric systems.

- **Identity Privacy:** Storage of biometric templates accompanied by other identity data results in significant privacy risks. The binding between biometric and other identity data allows malicious persons to link data subjects to applications beyond those using biometrics. Therefore, it is critical that the binding between biometric and other identity data is securely protected

- **Irreversibility:** To prevent the use of biometric data for any other purpose than originally intended, the biometric data should be transformed in such a way that the biometric sample cannot be retrieved from the transformed representation. Such transform should be irreversible, without compromising the biometric verification performance. Irreversibility should hold even when several biometric templates are accessible from different applications, services, or datasets.

- **Unlikability:** Tracking and tracing subjects across applications should be eliminated by ensuring that biometric templates used in various applications are unlikable. This guarantees that no adversary has a significant advantage over random guessing in determining whether two biometric templates are related or not; meaning that they were generated from the same source.

2.2.4 Security Requirements

- **Confidentiality:** Confidentiality ensures that information is not disclosed to unauthorized entities. In a biometric system, biometric data is stored and transmitted between various subsystems. Both storage and transmission of data should be protected against eavesdropping, unauthorized disclosure or modification of the data. This requires cryptographic techniques such as biometric encryption, or symmetric or asymmetric ciphers.

- **Integrity:** Integrity is the property of safeguarding the accuracy and completeness of assets in a given dataset. If the integrity of a biometric reference or the result of the various processing algorithms and subsystems are untrustworthy, the verification outcome will also be untrustworthy. Therefore, cryptographic means to protect the integrity of the data, such as signatures or authenticated encryption and time stamping, are required.

- **Renewability and revocability:** A strong security concern for biometric system relates to renewability and revocability of biometric templates. Individuals have a limited number of irises and fingers; identity theft renders corresponding biometric template as unusable for future use. Due to the persistence of biometric characteristics, a biometric template that is compromised once is compromised forever. The risk of compromised biometric templates can be mitigated for certain types of attacks by providing methods to allow renewable biometric templates. If various different biometric templates can be extracted from the same or similar biometric characteristic, the biometric template can be revoked and renewed in case it has become the subject of identity theft. [4]

2.2.5 Data Safeguarding Technique: Biometric Encryption

---

[3] Buhan, I. (2008) Cryptographic keys from noisy data – Theory and applications.
[4] Breebaart, J.; Yang, B.; Buhan-Dulman, I. ; Busch, C.: Biometric Template Protection. The need for open standards, (Datenschutz und Datensicherheit) 2009

The goal of data safeguarding is to mitigate the risks of malicious errors and attacks to the biometric dataset. Meeting the privacy and security requirements in a biometric system is a complex and elaborate task. Data safeguarding tools related to biometric data transformations have been published in the literature. These solutions are called biometric encryption or biometric template protection.

Biometric encryption is the process of using a characteristic of the body as a method to code or scramble/descramble data. Physical characteristics such as fingerprints, retinas and irises, palm prints, facial structure, and voice recognition are just some of the many methods of biometric encryption being researched today. Since these characteristics are unique to each individual, biometrics is seen as the answer to combat theft and fraud. Reason that this new technology is believed to be superior to the use of passwords or personal identification numbers (PINs) is that a biometric trait cannot be lost, stolen, or recreated. Encryption is a mathematical process that helps to disguise the information contained in messages that is either stored or transmitted in a dataset. There are three main factors that determine the security of the encryption system: the complexity of the algorithm, the length of the encryption key used to disguise the message, and safe storage of the key. Biometric encryption makes standard character encryption obsolete by replacing or supplementing the normal key characters with a personal identifier of the user that there can only be one perfect match for. Without this biometric key the information is inaccessible.

There are two broad categories of encryption systems; single key, or symmetric, systems and two key, or public, systems. Symmetric systems utilize a single key for both the sender and receiver for the purpose of coding and decoding data. In 1972, IBM developed DES (Data Encryption Standard) which was adopted worldwide by 1977 as the most common single key system. The process of transmitting this type of key over such networks as the Internet is one of the major failures due to the vulnerability of a single key system to interception. Data transmission may be conducted over open networks instead of dedicated networks and single key systems do not offer a high enough level of security for such transmissions. This issue of security led to the development of public key system. Two-key systems use a public key to encrypt the data and a private key to decrypt the data. The public key systems allows better encryption than single key systems, however certification of the recipient of messages becomes an issue, which causes a hierarchy of certification to be developed resulting in a much slower processing time. Biometrics can aid in this process due to the inherent nature of using a physical trait of the desired recipient to decipher the message.[5]

---

[5] http://www.emory.edu/BUSINESS/et/biometric/Biometrics.htm

3   Select Biometric Data Safeguarding Implementations

The rapid advancement of biometric technology along with the ease with which biometrics data can be acquired has resulted in the accumulation of large datasets of biometrics information. However, reporting of best practices has been minimal in regards to data sharing and safeguarding. This section provides an overview of biometric deployments in national and international jurisdictions with an assessment framework for decision-making on the issues surrounding data safeguarding. Critical areas assessed include system requirements, risk factors, strengths and weaknesses of the deployed data safeguarding technologies, privacy issues, and performance. The objective is to provide deployers and decisions-makers with the full range of information necessary to implement secure and interoperable solutions in defence and security applications.

3.1   Biometric Data Safeguarding Deployments by Application: Border Control

Border control is the use of biometrics to identify or verify the identity of individuals entering or leaving a border at a given time. The biometrics is used to complement authentication mechanisms such as passports and government-issued visas. Fingerprint is the most commonly deployed biometric technology in border control solutions, with iris and face recognition having gained much ground due to increased need for security in the recent years. Combination of these modalities is deployed for higher accuracy and greater flexibility.

3.1.1   U.S. Visitor and Immigration Status Indicatory Technology (US-VISIT)

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) is an immigration and border management system operated by the US Department of Homeland Security (DHS). The purpose of the program is to enhance the security of citizens and visitors, facilitate legitimate travel and trade, ensure the integrity of the US immigration system and protect the privacy of visitors. Put into operation on January 5, 2004, the program has been implemented across all major ports of entry within the United States including airports, seaports, land ports and US Consulates abroad. As one of the first full-scale mandatory biometric collection programs, US VISIT represents an excellent case study when considering the data sharing and safeguarding challenges associated with a large-scale data management system servicing multiple government organizations.

Biometric data is collected from foreign nationals when they apply for visas at US consulates in their respective countries of origin. The system captures ten fingerprints and a face image of every enrollee. Fingerprints are run

Figure 6: US-VISIT fingerprint collection[6]

against national datasets including the DHS Automated Biometric Identification System (IDENT) as well as the FBI's Integrated Automated Fingerprint Identification System (IAFIS) dataset in order to ensure that an individual does not have a previous criminal record and is not on a watchlist. Upon arrival to the US, foreign nationals provide fingerprint and face data again at all ports of entry as part of the verification process (see Figure 6) to insure that each individual is the same person to whom the initial visa was issued. The last implementation phase is collection of biometric data upon exit. DHS completed conducting pilot programs at 12 airports and 2 seaports and is implementing new biometric exit procedures based on these pilots for all non-U.S. citizens departing the United States as of 2010. US-VISIT is accessed by 30,000 users from federal, state, and local government agencies.

IDENT is the primary repository of biometric information held by DHS in connection with its several and varied missions, including the US-VISIT initiative. IDENT is centralized and contains biometric, biographic, unique machine-generated identifiers, and encounter-related data during collection by federal, state, local, and international agencies. Biometric data includes fingerprints and photographs. Biographical data includes name, date of birth, nationality, and other personal descriptive data. The encounter data provides the context of the interaction with an individual including location, document numbers, and reason fingerprinted. Unique personal identifier is a new

---

[6] Image extracted from U.S. Customs and Border Protection photographic archives

category of records used to link individuals with their encounters, biometrics, and other data elements. IDENT generates, stores, and retrieves data by unique number or sequence of numbers and characters in an effort to accurately identify and account for individuals upon all encounters with the system. The US-VISIT biometric data are currently in migration to conformance with ANSI/NIST-compliant format, specifically to extensible markup language (XML) as its primary data exchange method.

The dataset is protected through multi-layer security mechanisms at physical, technical, and administrative levels. DHS facilities are limited through physical access control measures, confidentiality of communications between agencies are ensured through authentication of sending parties, and US-VISIT data are accessed only by personnel screened through background investigations commensurate with the level of access required to perform the duties. In regards to data retention and disposal, the biographic and biometric data collected by US-VISIT for which the statute of limitations has expired for all criminal violations or older than 75 years are purged. Fingerprint cards, which are created for the purpose of entering records in the dataset, are destroyed after data entry.[7]

The US-VISIT program has garnered positive results. In fiscal year 2007, a total of 46,298,869 entries were recorded at air and sea ports. 235,857, or 0.5% of these entries, were identified as possible overstays due to no departure record. The manual vetting system led to 273 U.S. Immigration and Customs Enforcement arrests, and 11,685 biometric watch-lists were recorded at the port of entries, which included individuals with criminal histories. United States Citizenship and Immigration Services also utilized the system to screen those who apply for immigration benefits, creating 31,324 hits.[8]

3.1.2   EURODAC

EURODAC – European Dactyloscopie – is a multi-national fingerprint dataset for identifying asylum seekers and anomalous border-crossers. Its participants include all EU Member States in addition to Norway, Iceland, and Switzerland. The dataset was constructed in an effort to reduce asylum-seekers attempting to process simultaneous claims for asylum in more than one EU country (referred to as "asylum shopping"). It consists of a centralized AFIS system located in Luxembourg that enrolls the fingerprints of first-time asylum seekers. The enrolled fingerprints are then checked against existing records in the dataset to identify multiple asylum applications. Information stored on the EURODAC dataset includes the asylum seekers' fingerprints, date of submission, and country of first entry; it does not store names or photographs. Additionally, to ensure the protection and interoperability of transmitted data, the EU-wide system required the building of a secure network to transmit data between the Central Unit and the Member States. Additionally, the information is encoded and processed into ANSI/NIST-compliant format.

Privacy concerns and protection of traveler information has influenced the development and data usage requirements of the EURODAC dataset. The EURODAC dataset only associates asylum seekers' fingerprints to their date of submission, country of first entry, and not their actual names or face images. This process helps to only identify those individuals attempting to process simultaneous claims, and can limit the use of stored information for secondary purposes. The European Commission, however, proposed in July 2009 to allow Member States' law enforcement authorities and Europol access to the EURODAC dataset to help investigations into terrorism and other serious crimes. The proposal has been met with criticisms by privacy advocates who question its legitimacy and necessity. Additionally, the European Data Protection Supervisor (EDPS) argues that the proper balance between the need for public safety and the right to privacy and data protection must be met.

3.1.3   Biometrics Identification System (J-BIS) (Japan)

---

[7] http://www.dhs.gov/files/programs/gc1180020923182.shtm
[8] Figures extracted from: http://www.cis.org/vaughan/USVISITNumbers

Japan Biometrics Identification System (J-BIS) is an automated identification and clearance system. It was designed to identify and clear incoming visitors to Japan using fingerprint and face recognition technology (see Figure 7). The system came online in November 2007, paralleled with the announcement that all foreign visitors to Japan, including foreign nationals with permanent residency, are required to be fingerprinted for identification purposes upon arrival at entry points such as airports and seaports. Fingerprint data is captured and searched against a national watchlist dataset for any historical criminal activity.

The watchlist dataset stores a mixture of from one to ten rolled or plain fingerprints who are also of varying print qualities. The identification system supports 50 concurrent transactions with a maximum 10 seconds response time. J-BIS system adheres to the NIST's Wavelet Scalar Quantization (WSQ) Gray-Scale Fingerprint Compression Specification for data exchange. While a search using biographic information such as name and passport number can be used to retrieve information from the dataset, the immigration officers are solely responsible for visually verifying the biographic search results against the biometric data at various points of entry.

Figure 7: Japan J-BIS system[9]

3.1.4 The Five Country Conference (FCC) Protocol

In August 2009, the United Kingdom's Border Agency (UKBA) announced its agreement to share fingerprint information with the governments of Canada, Australia, New Zealand, and United States in an effort to combat against identity fraud. In addition to UKBA, the other immigration authorities involved international data exchange are the Department of Immigration and Citizenship (DIAC) in Australia, Citizenship and Immigration Canada (CIC) and the Canada Borer Services Agency (CBSA), the DHS in the United States of America, and Immigration New Zealand (INZ). The Under the data sharing agreement, the UK would be able to swap fingerprint information on foreign criminals and asylum seekers with other countries' respective fingerprint datasets, which are:

- The Immigration and Asylum Fingerprint System (IAFS) of UKBA
- The Biometric Acquisition and Matching System (BAMS) in Australia
- The Automated Fingerprint Identification System (AFIS) in Canada
- The IDENT System in the USA
- The Immigration Biometric System (IBS) of New Zealand

This provides officials the opportunity to identify and flag travelers attempting to evade identification from international and local authorities. Forum members of the Five Country Conference (FCC), who engage in ongoing strategic initiatives on immigration controls and border security, are responsible the development of this agreement. For the first year of the plan, each participating country was required to share 3,000 sets of fingerprints with the other partnering countries, with fingerprint sets increasing as the roll out progresses.

All of the data exchanged will be conducted under Secure File Share Server (SFSS) hosted by the government of Australia.[10] The data exchange happens in two stages. In the first stage, anonymized fingerprints with a unique reference number will be transferred for the purpose of searching against other countries' fingerprint datasets. The second stage of data sharing will take place only in the instance of a fingerprint 'match' being identified, which

---

[9] Image extracted from: http://biometrics.org/bc2008/presentations/150.pdf
[10] http://www.ukba.homeoffice.gov.uk/sitecontent/documents/aboutus/workingwithus/high-value-data-sharing-protocol/pia.pdf?view=Binary

transfers biographical and other relevant data between the country that supplied the fingerprints and the country that identified a fingerprint match. The unique reference number is assigned to create a search code for the second stage of data sharing in case a fingerprint match occurs, from which the code enables the country to ascertain what data will be relevant to transfer in respect of that person. The data element that will be shared upon matching are as followed:

- Date, location, and reason fingerprinted
- Last name, first name, any other names
- Date of birth, place of birth, nationality, and gender
- Travel document number
- Photograph, facial image, and/or scan of the travel document biodata page

Fingerprints exchanged under the Protocol will be destroyed securely once the matching has taken place, whether or not a match is achieved. On cases where fingerprints are found to match, the countries will exchange such other information as relevant, proportionate, and lawful to exchange for their immigration and nationality purpose.

3.2   Biometric Data Safeguarding Deployments by Application: Civil ID

Civil ID is the use of biometrics to identify or verify the identity of individuals in their interaction with government agencies for the purpose of card issuance, voting, immigration or employment background checks. Common civil ID applications include voter registration, national ID and biometric passports. Biometrics is used to complement or replace authentication methods such as document provision, signature recognition, and manual photograph inspection. AFIS, face recognition and fingerprint are three most deployed biometric technologies in civil ID applications, with iris recognition slowly gaining market share. Civil ID applications require systems capable of performing large-scale 1:N identification, with AFIS providing the accuracy and scalability when combined with other biometric modalities.

3.2.1   Gambia Biometric identification System (GAMBIS)

The Gambia Biometric Identity System (GAMBIS)[11] project is an integrated biometric identity system through which the government of Gambia captures biometric details for all citizens and aliens in the country. The Biometric Identity Card of the Gambia Immigration Department was launched on 18 August 2009, replacing its previous national identity card in circulation. Biometric data used by GAMBIS is thumbprint based, and applicants are required to submit both thumbprints at the time of enrollment. Additionally, card issuance requires citizens to present their birth certificate, Gambian passport, and certificate of registration, voter's card, Seyfo certificate, village Alkalo's certificate or certificate of naturalization. An individual's data, including their biographic and biometric information is matched and captured in the national dataset. A National Identification Number (NIN), unique to each applicant's fingerprint, is issued in conjunction. As the country's next generation identification card, it enables its citizens and residents to confirm their identity based on their fingerprint and/or face data. Biometric documents issued for Gambia include national identity cards, residential permits, non-Gambian ID cards, and driver's license.

The GAMBIS project is one of the first biometric identity systems to issue multiple biometric identity documents, such as identity cards, passports, driver's license, visas, under one platform by combining all these documents in a national population dataset. The project and data enrollment operates out of eight GAMBIS branches and four mobile units. As of March 2010, near 70,000 National IDs, 7,000 Residential Permits, 20,000 National Driving Licenses have been issued through the GAMBIS project. [12]

3.2.2   The Bangladesh Voter Registration Project

---

[11] http://www.gambis.gm/
[12] http://www.gambis.gm/news.html

The Bangladesh Election Commission (BEC), in partnership with the Bangladesh army, established the Bangladesh Voter Registration Project to digitally register all legal voters in the country in advance of general elections in December 2008. The biometric registration of voter included collection of fingerprint and facial records. By the project's completion in October 2008, the project resulted in a dataset of 80 million registered voters using face and fingerprint technology, creating the world's currently largest biometric dataset. A portion of enrolled population was illiterate and/or had no previous identification documents. The project completion included the following eleven stages: Form distribution and data collection, data verification, data entry, data export to server, proof reading and editing, verification of proof voter list and handing over, ID card preparation, ID card distribution, correcting mistakes on ID cards, preparation of draft voter list and distribution, and data safeguarding and distribution. The system includes an integrated large scale AFIS and multiple biometrics face-fingerprint recognition system developed jointly by TigerIT Bangladesh Ltd and DohaTech. The resulting ID cards include a barcode encoded with ISO fingerprint templates and PKI digital hash printed on each card including name, gender, birth date, picture, signature, and fingerprint images.

The national identity dataset of Bangladesh contains the biometric and personal data of more than 80 million people, which raises privacy and security concerns. In January 2010, the National Identity Registration Bill 2010 was passed, which authorized BEC to become the custodian of this national dataset with power to inquire for any individual or institution for personal data. Notably, the law does not provide any clause for protecting the privacy of personal information, which enumerates the lack of privacy laws in Bangladesh today.

3.2.3   National ID Card (Thailand)

In April 2005, the Thai government contracted Precise Biometrics for a National ID card solution. Precise's Match-on-card technology was chosen and integrated by Smart Card System International Co. Ltd. The smart ID cards include digital fingerprint information thereby physically tying the card to a specific individual. The matching of the fingerprint takes place inside the card, not in the reader. The initial deployment included the supply of 12 million cards and 36,000 fingerprint readers, and was expanded in 2006 to include 64 million citizens. As of January 2007, 10 million ID cards were in use by Thai citizens. In addition to the traditional usage, the ID cards will be used in different contexts, such as in education and government ID cards.

The establishment of Thai national identity dataset raises both privacy and security concerns regarding data sharing and safeguarding methods. By the project's completion, Thailand's national ID dataset will grow in similar scale to the dataset of Bangladesh. In addition to the fingerprint information, the dataset ties the biometric information with the individual's other personal data such as the Population Identification Code, a 13-digit string of numbers assigned at birth or upon receiving the citizenship. With the increased adoption of biometric technology in national ID and biometric passport applications across the globe, the need for adoption of standardized of data security and exchange methods has become a pressing concern.

3.3 Biometric Data Safeguarding Deployments by Application: Criminal ID

Criminal ID is the use of biometric technologies to identify or verify the identity of a suspect, detainee, or individual in a law enforcement application. Criminal ID systems often include a large-scale biometric dataset. Typical criminal ID applications include executing fingerprint searches against local, state and national datasets as well as processing face images in the form of mug shots against datasets. AFIS is the dominant biometric technology in this space, followed by face recognition and fingerprint.

3.3.1 Multilingual Automated Registration System (MARS) (United States)

The Multilingual Automated Registration System (MARS) provides similar capabilities as that of the Biometrics Automated Toolset (BAT) with the addition of flexible multilingual user interfaces; the added user interface with additional languages is intended to aid in the transition process as U.S. forces implement the application locally to

Figure 8: MARS Work Station at the Rusafa Prison

Iraqi officials and military. As a user identification application, MARS provides fingerprint, face, and iris enrollment and identification capabilities along with digital entry of data and related identity information. The application is also designed to be compliant with FBI and Department of Defence (DoD) biometric enrollment criteria to better ensure interoperability of biometric data.

As illustrated in Figure 8, a number of biometric capture devices are attached to a single laptop to allow operators to capture multiple biometrics from detainees. A COTS digital camera is utilized to capture multiple headshots and face shots from each detainee for face recognition; typical face captures include front image, left and right side 90 degree side profile, and left and ride 45 degree side profile. In addition, the system collects the individual's fingerprint, thumbprint, and iris images.

One of the first deployments of the MARS registration system was established in March 2009 at the Rusafa Prison, Baghdad and operated independently by Iraqi officials. The solution included a complete end-to-end architecture that allowed for multimodal biometric identification and enrollment of detainees. At the designated prison facility, the solution was able to enroll a population of over 25,000 detainees even when operating continuously over an extended period of time.

The solution was also designed to access external, centralized datasets to obtain real-time information about detainees and facilities. MARS creates Electronic Biometric Transmission Specification (EBTS) files to be shared with the DoD authoritative biometric repository, the DoD Automated Biometric Identification System (ABIS). These files can subsequently be shared through the DoD ABIS with interagency partner systems such as the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System (IAFIS) enabling effective global identity management. In addition, the system features the capability to create Biometric Data files (BDF) for storage and exchange of biometric and demographic data. The file permits creation of digital dossiers within the enterprise linking identities and situational information. MARS features a scalable client-server architecture from which the Detention Management System (DMS), a web-based detention and prison management system, exchanges information. MARS serves as the enrollment point for detainees and manages their detained status, while DMS connects to MARS or BAT to update its knowledge of persons in the system. The system provides real-time data exchange about detainees and facilities is available for management purposes from one central location using DMS Portal, a web-based portal providing detention and prison oversight capability.

3.4 Biometric Data Safeguarding Deployments by Applications: Surveillance

Surveillance is the use of biometric technologies to identify individuals present in a given space or area. Biometrics is used to complement or replace authentication methods such as manual monitoring of cameras. Surveillance applications scan crowds and open spaces, capturing faces in a field of view from a variety of angles without the end-user knowingly interacting with a camera. Surveillance applications are classified by covert operations and its real-time 1:N functionality. Face recognition is the only technology used in surveillance due to its ability to acquire non-cooperative subjects from a distance and the existence of facial watchlist datasets.

3.4.1 New Delhi Railway Station Face Recognition Surveillance (India)

In January 2005, the New Delhi Police initiated a facial recognition surveillance pilot program at the New Delhi Railway Station (see Figure 9). The system, similar to those deployed in Dubai and Singapore, includes cameras and searchlights installed at the entry and exit points of the station. The system processes each person as they enter and exit the station and runs the picture against a criminal dataset of most-wanted criminals. If a matching record is found, the cameras begin recording.

The facial recognition system is connected to a control room set up at the station where two computers—the recorder and server—will process the pictures for a scan against the watchlist dataset in the server. The server is equipped with software containing the photographs of most-wanted criminals and it flashes a signal if the system finds a match in the records. The surveillance system can analyze 20 photographs simultaneously. The frequency of synchronization with the national criminal dataset is unknown. The system has been installed to increase traveler security and to also reduce surveillance camera film costs, as the cameras only begin recording when there is an observed threat.

Figure 9: New Delhi Railway Station

3.4.2 Community Protection Face Recognition System (United Arab Emirates)

Community Protection Face Recognition System is a part of United Arab Emirates (UAE) Ministry of Interior's Community Protection initiative, which aims to implement a comprehensive national critical infrastructure protection system. One part of that system that is currently in place is a biometric watchlist based on iris recognition, called the Iris Expellee Tracking System (IETS) used to prevent illegal entry at UAE ports and to recognize wanted criminals. The face recognition system complements the more narrowly focused iris system to perform identification checks of entrance and people in transit lounges. The system features real-time facial capture and enhancement technology and automated identity searches upon matching against criminal records. Its advanced detection technology instantly locates key facial characteristics during enrollment process for immediate analysis. Plans are in place for the system to be integrated into the passport control system of the Dubai Naturalization and Residency Department.

The underlying biometric technology selected for the face recognition system is to be provided by CryptoMetrics, Inc., a global biometric technology vendor. CryptoMetrics and the Ministry of Interior have entered into a 25-year exclusive partnership, along with BioDentity Systems LLC, to deploy face recognition systems in UAE. Face recognition enrollment images will be in compliance with standards of the International Civil Aviation Organization (ICAO). The system has been deployed at Abu Dhabi International Airport since July 2008. As of November 2008, four units were soon to be introduced at Dubai International Airport. Two more are planned for the exterior of the airport in Dubai, and there are plans to expand the system to all UAE ports of entry, including the Fujairah and Ras al-Khaimah airports. The plan is to have four face recognition sites at important ports of entry.

The system allows critical identification checks to be performed from a distance without a person's active participation. The system also helps inspectors at control points inside the airports to facilitate the clearance of

persons without inconvenience or delay to the passengers while implementing continuous and proactive checks designed to immediately detect persons who should be denied entry or detained.

3.5   Data Safeguarding in Canadian Security Deployments

New biometric technologies and its associated data safeguarding capabilities must consider existing programs and data sharing and safeguarding protocols currently in place. This section provides an overview of current Canadian biometric deployments in security applications and assesses the effectiveness of information exchange and biometric dataset safeguarding practices in existing applications.

3.5.1   CANPASS

CANPASS (Canadian Passenger Accelerated Service System) is a joint initiative of the Canada Border Services Agency (CBSA) and Citizenship and Immigration Canada (CIC) designed to streamline customs and immigration clearance into Canada for pre-approved, low-risk frequent travelers. The program was initiated in November 2004 to serve airline passengers, but has since expanded to include both air and marine travel. Pre-approved travelers with CANPASS provide their iris images to confirm their identities against an issued identification card used at self-service kiosks located within international airports (see Figure 10). Participating Canadian airports include the Calgary International Airport, Edmonton International Airport, Halifax International Airport and the Vancouver International Airport. The CANPASS program consists of a variety of iterations customized for specialized border crossing scenarios, including via corporate aircraft, private aircraft, private boats, and in remote areas. There are currently almost 4,800 approved CANPASS travelers.

Figure 10: CANPASS trusted traveler program

Once an applicant has completed and signed the CANPASS application form, the CBSA is authorized to collect personal information such as name, date of birth, address, citizenship, proof of citizenship and residency information.

The information will be used for background security checks and is not shared with a third party. All information is stored in a secure central dataset, which in turn is protected by various methods, including firewalls. Access to client information by employees is also controlled and monitored.
All personal information provided is protected under the federal Privacy Act of Canada.

3.5.2   NEXUS

NEXUS is a joint program between the U.S. Customs and Border Protection (CBP) and Canada Border Services Agency (CBSA), which facilitates the simplified security processing for pre-approved travelers. The program was originally established in 2002 as part of the Shared Border Accord between the United States and Canada, and has since expanded to include the management of travel lanes at airports, waterways, and land crossings. NEXUS biometric data consists of digital fingerprints, iris scan, and a facial photograph.

Additionally, membership with NEXUS fulfills the travel document requirements of the Western Hemisphere Travel Initiative (WHTI) that requires all U.S. and Canadian citizens to hold a government issued passport or other secure travel document when seeking entry or re-entry into the U.S. by air. There are currently 383,000 approved travelers in the NEXUS program, which has been implemented at 16 border crossing locations, 33 marine locations in the Great Lakes and Seattle, Washington regions, and eight international airports in Canada, including Vancouver International Airport, Toronto Pearson International Airport, and Calgary International Airport. NEXUS self-service kiosks employ iris recognition technology to quickly screen travelers, allowing them to bypass customs and immigration lines. Enrollment in the program consists of a basic background check, fingerprint capture, and iris

capture. Membership lasts for 5 years. As of January 2011, all NEXUS members can utilize Global Entry Kiosks at participating airports.

Applicants are screened for citizenship and immigration status, checked for criminal history and positive matches on U.S. Federal Bureau of Investigation (FBI), Canadian Security Intelligence Service (CSIS), Royal Canadian Mounted Police (RCMP), United Nations, and Interpol terrorism and no-fly list datasets and United Kingdom Police National Computer. The information provided by each applicant, including supporting documentation and biometric data, is collected under the Customs Act and is protected under the Privacy Act. The information will be used to make a determination of your application and the operation of the programs, and are shared with other government agencies in Canada and the United States of America. Finally, the information will be retained in the Personal Information Bank #CBSA PPU 031, which could be obtained by participants of the program.

Since the NEXUS air and land programs were merged in 2007, interest in the CANPASS program has declined, since NEXUS provides a broader range of services at the same price, including both expedited Canadian and U.S. immigration at Canadian airports. The most likely reason an individual would be inclined to use CANPASS rather than NEXUS is because he or she is deemed ineligible for NEXUS by the United States.

4 Biometric Privacy-Enhancing Techniques

4.1 Introduction

Experts in biometrics and information security widely recognize the danger of processing, transmitting, and storing biometric information in the clear. Biometric templates are sensitive representations of their owners, and the theft or misuse of them can incur serious injury. International standards on the secure management of templates have matured insofar as how they are stored and transmitted. Match-on-card technologies and other client-side matching devices have taken to the market recently, illustrating the progress of biometric data safeguarding technologies. Ironically, there remains to be a definitive agreement on how to store biometric templates in a format that secures their owners from identity theft in the event that the templates are stolen.

Biometric template protection methods are processes by which biometric templates are transformed into pseudonymous identifiers of their owners. Reliable pseudonymous identifiers are secure and robust, preserving the anonymity of their owners while reliably distinguishing them from other individuals. Such processes represent a mere step in the flowcharts most security protocols, but arguably they uphold privacy in biometric systems at a most fundamental level. Thus biometric template protection methods are continuing to mature in a rigorous academic debate as they have been for about a decade. Commercial and governmental organizations have not yet widely adopted template protection methods in their existing biometric products or systems; however a handful is investing in the research and development of such methods.

This report describes many template protection methods that have matured in the academic discourse. These methods are not mutually exclusive, but for organizational purposes they are divided into loose categories. Each overarching method is introduced with an overview that covers its general methodology, known vulnerabilities and defence strategies, and typical performance rates. Security vulnerabilities are analyzed insofar as they pertain to the privacy of the user, whereby the inversion of a protected template would compromise the confidentiality of the user's identity. Commercial developments in template protection are reviewed separately from those in academia. The bibliography lists references for every article and patent reviewed in this report and lists other relevant articles not necessarily reviewed or referenced in the report, such as attack strategies on well known template protection methods. Appended to the report is a summary of the test results for every empirical study reviewed.

4.2 Summary of Approaches

Figure 11 summarizes the approaches examined for this Study.

Article	Method	Notes
Al-Assam et al. (2009)	Projection	Reduced the projection method to two steps, eliminating the need for the commonly used Gram-Schmitd algorithm.
Álvarez et al. (2009)	Fuzzy	Produced vault sets that were resistant to cross-matching by salting the minutiae point coordinates with a secret key.
Ang et al. (2009)	Transform	Produced cancelable biometrics by using a revocable key in the transform function.
Ballard et al. (2008)	Multifactor	User password and random oracles influenced the generation of keys to improve entropy, regardless of modality.
Barbosa et al. (2008)	Homomorphic	Salted keys with random oracles to improve entropy.
Barni et al. (2010)	Homomorphic	Borrowed elements of Paillier and ElGamal cryptosystems using elliptical curves to save bandwidth during encryption.
Boult et al. (2007)	Transform	Divided input biometric into stable and unstable bits, encoding the stable and preserving the unstable to aid authentication. Minimized tradeoff between security and performance.
Chen and Chandran (2007)	Transform	Applied an iterative, bispectral transform and Reed-Solomon error correction codes.
Chen et al. (2009)	Parametric	Generated keys from statistical measurements of input behavior.
Chikkerur et al. (2008)	Projection	Generated signatures from local image patches around minutiae points rather than their coordinates. Required no alignment of the minutiae.
Clancy et al. (2003)	Fuzzy	First biometric implementation of fuzzy cryptosystem.
Costanzo (2004)	Parametric	Generated cryptographic keys from the aggregation of parameterized measurements. Original biometric data not used to produce the keys.
Freire-Santos et al. (2006)	Fuzzy	Introduced automatic alignment of fingerprint images.
Hao et al. (2002)	Parametric	Developed a PKI system that produced keys from encrypted biometric templates.
Hao et al. (2006)	Multifactor	Produced nearly error-free codes by preprocessing biometric data with Reed-Solomon and Hadamard codes.
Hirata and Takahashi (2009)	Transform	Applied minimum average correlation energy filters to produce templates that were comparable in the encrypted domain. 0% EER reported.
Huang et al. (2011)	Homomorphic	Server gains no knowledge of the raw input data. Among the most computationally efficient methods.
Jin et al. (2009)	Aggregation	Generated bit strings from the angle and occurrences of minutiae within random triangles.
Kanade et al. (2010)	Multifactor	Improved entropy by preprocessing biometric data with Reed-Solomon and Hadamard codes and salting key with password.
Linnartz and Tuyls (2003)	Fuzzy	Introduced delta-contracting and epsilon-revealing functions to produce anonymized representations of the original biometric.
Maiorana et al. (2008)	Transform	Used hidden Markov models to compare templates in the encrypted domain.
Merkle et al. (2010)	Fuzzy	Exponentially improved the entropy of vault sets by superimposing data from multiple fingerprints.
Monrose et al. (2001a)	Multifactor	Authentication based on password and keystroke behavior. Decision made in a single input. Adapted to changes in behavior over time.
Monrose et al. (2001b)	Multifactor	Authentication based on password and voice measurements. Decision made in a single input. Adapted to changes in behavior over time.
Nagar et al. (2009)	Fuzzy	Improved entropy and matching performance by including minutiae descriptors in the vault sets.
Nagar et al. (2010)	Aggregation	Extended the method of Sutcu et al. (2008) to include fingerprint ridges.

Article	Method	Notes
Nandakumar et al. (2007)	Fuzzy	Produced cancelable vaults by salting them with user-supplied passwords.
Nandakumar and Jain (2008)	Fuzzy	Produced multimodal vault sets to exponentially improve the entropy of vault sets.
Ŏrencik et al. (2008)	Fuzzy	Developed an algorithm that arranged chaff points in a more realistic manner than uniform randomness.
Ouda et al. (2010)	Projection	Randomly mapped consistent bits of biometric data to encode cryptographic keys. Keys could be cancelled by changing the value of the random seed.
Rane et al. (2009)	Homomorphic	Extend the method by Sutcu et al. (2008), applying Slepian-Wolf syndromes and LDPC codes on irises and fingerprints.
Scheirer and Boult (2008)	Transform	Generated tokens that can be re-encoded to form hierarchies of trust, in the same way certificate authorities issue digital certificates.
Scheirer and Boult (2009)	Transform	Only reliable bits stored in the vault set. Allegedly resistant to rotations and translations among inputs.
Shi et al. (2008)	Transform	Plotted minutiae points on a polar coordinate system, centered on a region of interest.
Soutar et al. (1999)	Transform	Transformed fingerprint images rather than features. Produced keys usable in AES.
Sutcu et al. (2007)	Fuzzy	Improved matching performance by quantizing the input and mapping the coefficients to discrete domains prior to constructing the vault set.
Sutcu et al. (2008)	Aggregation	Generated bit strings from the occurrences of minutiae within random cuboids. Implemented Slepian-Wolf syndrome codes.
Takahashi and Hirata (2009)	Transform	Developed an image chip matching algorithm that uses correlation invariant random filters.
Teoh et al. (2007)	Projection	Applied multispace random projections to the method by Teoh et al. (2004), preserving security in stolen-token scenarios.
Teoh et al. (2004)	Multifactor	Minutiae coordinates and tokenized random number influenced cryptographic key generation. 0% EER reported.
Uludag and Jain (2006)	Fuzzy	Appended a checksum to the vault set, eliminating the practical need for error correction codes.
Van der Veen et al. (2006)	Fuzzy	Optimized the fuzzy vault scheme for use by machine readable travel documents.
Vielhauer et al. (2002)	Parametric	Generated cryptographic keys from parameterized measurements of biometric inputs. No original samples saved.
Yang et al. (2010)	Projection	Revised method by Teoh et al. (2007) to support dynamic and nonlinear projections, improving resistance to reverse engineering.
Ye et al. (2009)	Homomorphic	Implemented k-anonymity to prevent the server from directly examining the input biometric.
Zheng et al. (2006)	Fuzzy	Introduced lattice mapping as an alternative means for constructing vault sets.

Figure 11: Summary of Biometric PETs Evaluated in this Study

4.3 Fuzzy Cryptosystems

A "sketch" or "vault" is a secured template whose development can be traced to the "fuzzy vault" scheme proposed by Juels and Sudan (2002). The scheme was designed to encrypt data such that it could be unlocked by similar but inexact matches. Variants of the fuzzy vault scheme are referred to more generally as fuzzy cryptosystems. The method lent itself well to the protection of biometric templates, where inputs are inconsistent due to lighting, rotation, etc. The mechanism for obfuscating data in fuzzy cryptosystems is to insert random noise that resembles genuine minutiae points or other features. In doing so an attacker cannot easily differentiate genuine features and false features. Most variations of this system follow key release protocols, though some generate keys from the biometric data. The key generation variant was pioneered by Dodis et al. (2008) and is often referred to as a "fuzzy extractor." Fuzzy cryptosystems are perhaps the most practiced and debated template protection methods in academia. As a result there is a wealth of literature on the security vulnerabilities and countermeasures to mitigate these vulnerabilities, making this method among the most mature of all template protection methods despite its many shortcomings.

Given its inherent weakness to collusion attacks, fuzzy cryptosystems should be employed only in an environment where access to the template storage device is reliably secure. Furthermore they are better suited for applications that enroll multimodal biometrics. This ensures that the vault set retains a high level of entropy to resist brute force attacks. Applications endowed with greater computing power should consider alternative template protection methods that offer a greater level of security at the expense of computational efficiency. To the extent possible given practical constraints, a fuzzy cryptosystem should make use of the strategies proposed by Poon and Miri (2009) and Mihãilescu (2007) to harden the vault set against collusions attacks and brute force attacks.

4.3.1 Method

Three steps generally constitute the protocol for fuzzy cryptosystems:

- **Feature extraction**

Biometric feature data are recorded onto a set that represents the original or "genuine" biometric features. This is referred to as the genuine set. Among the articles reviewed, the most widely adopted structure for this set consisted of the coordinates and angles $m_i=(x,y,\theta)$ of fingerprint minutiae. The ordinate values of the minutiae points are encrypted by a secret polynomial p.[13] A genuine set G of n minutia points m_n is expressed verbosely as

$$G=(m_1,m_2,...m_n)=((x_1,p(y_1),\theta_1),(x_2,p(y_2),\theta_2),...,(x_n,p(y_n),\theta_n))$$

- **Noise generation**

Random data is recorded onto a set that represents counterfeit biometric features. This is referred to as the "chaff" set. The chaff set serves as a decoy, such that anyone reading the template could not easily distinguish genuine points from chaff points. To be effective, it must be structured in the same fashion as the genuine set but should contain many more points to augment the entropy of the vault set. The number of chaff points that can be generated without ruining verification performance is limited by the size of the image. A chaff set C of i chaff points c_n is expressed verbosely as

$$C=(c_i,c_i...c_n)=((x_1,p(y_1),è_1),(x_2,p(y_2),è_2),...,(x_i,p(y_i),è_i))$$

- **Point Shuffling**

The genuine and chaff sets are combined and shuffled by a function S to create a secure set, referred to in the literature as a vault or sketch. A vault set V of $n + i$ points v_n+i is expressed verbosely as

---

[13] In a coordinate pair (x,y), y represents the ordinate.

$$V=(v_1, v_2, \ldots v_{n+i}) = S(G \cup C) = S((g_1, g_2, \ldots g_n), (c_1, c_2, \ldots c_i))$$

The system must decode the sketch before it can match the data against inputs. First it must distinguish the genuine data from the random noise. It achieves this through polynomial reconstruction, which typically requires the use of error correction codes and "helper data." Typically the similarity between an input and a stored template is scored by measuring their Hamming distance.

4.3.2 Vulnerabilities[14]

Collusion Attacks

Early fuzzy cryptosystems were not inherently revocable. An attacker could compare the abscissa values[15] between two vaults generated from the same fingerprint to identify the genuine points in both vault sets. If an attacker is capable of breaching one dataset and stealing data, it should be assumed that the attacker can breach other datasets. An attacker that obtains vault sets from multiple datasets can identify which points are genuine by comparing the sets against those in other datasets. While the chaff points will be different for two vault sets from the same user, the abscissa values of the genuine points will always be the same; thus the genuine points are suggested by their consistency among vault sets across multiple datasets.

Poon and Miri (2009) designed algorithms for executing collusion attacks on fuzzy cryptosystems, which assumes that an attacker has access to multiple vaults locked by the same fingerprint stored on multiple datasets or smart cards. The attack involves the comparison of points across multiple vault sets and singles out the points which appear in more than one vault. By a process of elimination, the size of the vaults can be reduced until the remaining points are deemed genuine with a high degree of confidence. The researchers proposed several strategies for mitigating the risk of collusion attacks, one of which was to apply a one-way transform to the vault set.

Nandakumar et al. (2007) proposed a variation of the fuzzy cryptosystem that mitigated collusion attacks by using multifactor authentication, using a password or token to alter the key generation process.

Brute Force Attacks

The application of a fuzzy cryptosystem on a fingerprint image typically produces low entropy vault sets. This makes the templates susceptible to brute force attacks and incompatible for use as cryptographic keys in common security protocols like AES, which require a minimum key length of 128 bits. Mihãilescu (2007) analyzed the ability of fuzzy cryptosystems to resist brute force attacks. While the seemingly obvious solution would be to generate more chaff points, the researcher noted that the number of chaff points that can be generated is limited both by the size of the image and by the variance of the genuine minutiae points. The researcher proposed several strategies for mitigating the risk of brute force attacks: (1) enroll multiple fingerprint images to augment the entropy of the vault set exponentially; (2) generate a non-random distribution of chaff points by laying a hexagonal grid on the fingerprint template, such that each grid point is associated with a point, be it chaff or genuine.[16]

The means of maintaining data integrity some variations of the fuzzy cryptosystem opened the door to brute force attacks. Uludag and Jain (2006) and Nandakumar and Jain (2008) appended a checksum to the vault set which allowed the server to determine if a match was successful more efficiently. Mihãilescu (2007) observed that while this method enhanced system performance, it would allow an attacker to understand in real time when an attempted brute force attack succeeds. To use checksums therefore facilitates the execution of offline brute force attacks.

---

[14] Researchers have also identified another vulnerability whereby an attacker can substitute some of the chaff points in the vault set with his or her own genuine points, thus enabling the system to recognize the attacker as legitimate. While this is concerns the security of the method, it does not concern the privacy of the user and therefore falls outside the scope of this report.

[15] In a coordinate pair (x,y), x represents the abscissa value.

[16] See Mihãilescu (2007): 7-8.

Nandakumar and Jain (2008) and Merkle et al. (2010) proposed the enrollment of multiple fingerprints and multimodal biometrics to exponentially increase the size of the vault set. The multiple fingerprint vault set, which performed better than the multimodal vault set in a test by Nandakumar and Jain (2008), achieved a size of 224 bits where the error rates were lowest. Unfortunately the solutions proposed in both publications would be unacceptable in most existing fingerprint applications, which were designed to enroll and match a single fingerprint image.

Information Leakage

Most fuzzy cryptosystems store public auxiliary information, referred to in the literature as "helper data," to reduce intraclass variance, thereby enhancing the verification performance of the system. Helper data derives from the original biometric input. Uludag and Jain (2006), for example, used the maximum curvature points and the corresponding curvature values from the orientation flow curves of the minutiae. The caveat is that the helper data leaks trace amounts of information on the original biometric, making it easier to reverse engineer the original biometric from the vault set. Most researchers claimed that the amount of information leaked is trivial, but the security risk should be assessed nonetheless.

4.3.3 Performance

Empirical tests on the performance of fuzzy cryptosystems have produced mixed results. Researchers have applied the method to face, iris, fingerprint, signature, ear, and multimodal biometrics. None of the key binding variations met the performance target of 1% FRR at 0.1% FAR, and only one key generating variation met the target. Van der Veen et al. (2006), whose method was eventually developed into an algorithm now sold in products by priv-ID, achieved the best results using a key binding variation against face images at 0.25% EER. An implementation of the method by Linnartz and Tuyls (2003) yielded the best results using a key generating method against ear biometrics at 0.6% FRR at 0.05% FAR, which meets the performance target. Ironically, as researchers invested so much time in the development of fuzzy cryptosystem for fingerprints, the method has yet to produce acceptable performance rates for that modality.

4.3.4 Articles

Clancy et al. (2003)

At the time of this publication, smartcards had become a common technology and concerns grew over the security of private keys stored in the cards. Clancy et al. proposed a framework for a smartcard system in which the private key was encrypted and decrypted by an authorized fingerprint. The proposed method was the first variation of the fuzzy vault scheme by Juels and Sudan (2002). Referred to by the researchers as a "fingerprint vault," the proposed method used the coordinates of fingerprint minutiae to encrypt and decrypt the private key.

Method

For each transaction the user presents a fingerprint image from which a vector of features are extracted. For the purpose of this paper, the researchers treated the extraction and alignment of features as a black box. The minutiae coordinates $m_i=(x_i,y_i)$ form the basis of the key used to lock the vault. To handle intraclass variations, a matrix of

likely minutiae locations $(\bar{x}_i,\bar{y}_i)$ from a given minutiae set is constructed using an additive Gaussian noise model.

Chaff points are added to obfuscate the fingerprint data. To prevent quantization errors, the chaff points must not be placed too close to the genuine points or to themselves. The researchers use a circle packing algorithm to generate as many chaff points as possible within the limited space while maintaining sufficient randomness.

During enrollment, the user presents N fingerprint images resulting in N minutiae sets, b1,b2…bN. To derive the locking set L, let A be the set of average points with multiplicity. For each minutiae mi in each set bn elements are

selected from nk ∈ A where |nk-mk|<T. If no matches are found, mj is added to A with a multiplicity of one;

otherwise mi is added to the average and the multiplicity is increased such that A={a ∈ A: multiplicity(a)>S}. Figure

12 illustrates how the reliable minutiae point regions are determined after several training enrollments.

During authentication, the user presents a single fingerprint image from which a minutiae set U is derived. For each point in the set, the system finds the closest point in the vault set. They used the Berlekamp-Massey algorithm, a variation of Reed-Solomon decoding, to unlock the vault. The secret polynomial can be reconstructed if at least (ä+n)/2 points in the query set match a genuine point in the vault set, where ä represents the radius of the reliable minutiae regions.
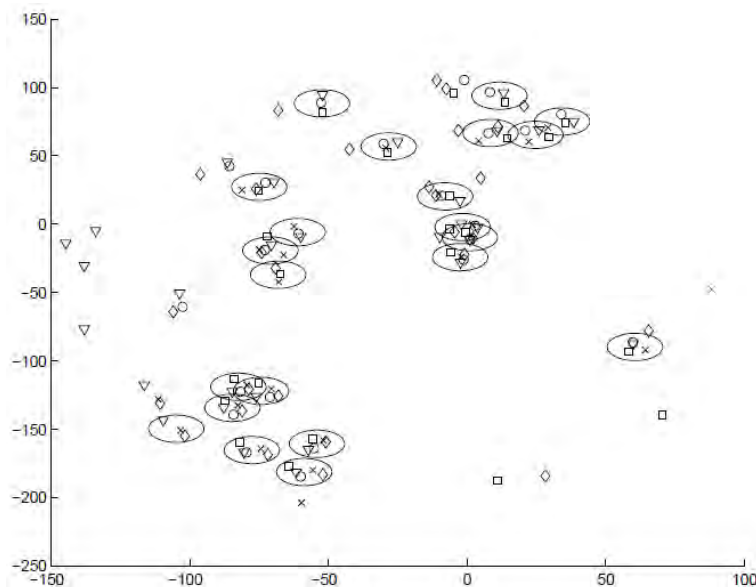
Figure 12: Example of reliable minutiae regions   after five fingerprint scans

Performance

The researchers tested the proposed method against fingerprint images. They achieved ~30% FRR at ~0% FAR, which is unacceptable in many applications. False match rates and false non-match rates rose as the polynomial degree and number of chaff points rose. Uludag et al. (2004) noted that this method required fingerprint images to be pre-aligned in order to perform well and that it was not tested in a sufficiently realistic environment.[17] Therefore the method required significant tuning, as would happen in the development of the fuzzy cryptosystem.

Linnartz and Tuyls (2003)

Linnartz and Tuyls were concerned with the unauthorized collection and misuse of biometric templates, which at the time were often stored in the clear. They attempted to obfuscate templates as a means to safeguarding the privacy of their owners. The proposed method used transform functions to irreversibly anonymize biometric information. Their study was the first to concern itself not just with the ability to produce cryptographic keys from biometric data but to

---

[17] Umut Uludag et al., "Biometric Cryptosystems: Issues and Challenges," *Proceedings of the IEEE* 92 (2004): 956.

safeguard the privacy of biometric data. The theory behind the methodology was foundational to the work of Dodis et al. (2008).

Method

At a high level, a feature measurement Y is extracted from the biometric image that a user presents upon enrollment. A signal processing function G=(W,Y) quantizes the supplied information to reduce noise. The refined data Z=G(W,Y) is then obfuscated by a hash function F to produce a secure, noninvertible template U=F(Z). The signal processing function G is applied to the input data to ensure that the input values are mapped to the same values as those in the stored template.

For the ith dimension $(1,2,\ldots i,\ldots,n_l,n_l=n_2)$ of Y, W, and Z the δ-contracting function is expressed as

$$z_i = \begin{cases} 1 \text{ if } 2nq \leq y_i + w_i < (2n+1)q \text{ for any } n = \cdots,-1,0,1 \ldots \\ 0 \text{ if } (2n-1)q \leq y_i + w_i < 2nq \text{ for any } n = \cdots,-1,0,1 \ldots \end{cases}$$

where q is the quantization step size and w is the watermark of quantization index modulation.[18] During enrollment, x_i is measured and the certifying authority finds a w_i such that the value of $y_i + w_i$ is pushed to the nearest lattice point where $x_i+w_i+ä$ is quantized to the same z_i for any small ä .The watermark w is expressed as

$$w_i \begin{cases} \left(2n+\dfrac{1}{2}\right)q - x_i & \text{if } s_i = 1 \\ \left(2n-\dfrac{1}{2}\right)q - x_i & \text{if } s_i = 0 \end{cases}$$

where n=⋯,-1,0,1… is chosen such that –q < w_i < q. The value of n is discarded while the values of w are used as

helper data in subsequent transactions.

Performance

The researchers discussed the theory behind the proposed method in theory but did not test empirically. But it was implemented in a subsequent study by Tuyls et al. (2004), who tested the proposed method against 360 ear images from 45 unique individuals. They achieved 0.6% FRR at 0.5% FAR where mean key length l = 370 and ä=2.0. These are the best results achieved by a fuzzy cryptosystem among those review in this report. They observed that FRR falls as either ä or key size *l* rises, and the key length *l* falls as ä rises.

Van der Veen et al. (2006)

Van der Veen et al. proposed a variation of the fuzzy vault scheme by Juels and Sudan (2002) intended for use in machine readable travel documents. The proposed method was one of the few fuzzy cryptosystems to be applied to a modality other than fingerprints, yet it was among the best performing variants reviewed in this report. Van der Veen is now the CEO of priv-ID, a leading provider in privacy enhancing technologies for biometrics, and the other researchers in the report have filed multiple applications for patents on biometric template protection.

Method

---

[18] The researchers cite B. Chen and G.W. Wornell, 1998, "Digital Watermarking and Information Embedding Using Dither Modulation," in *IEEE Workshop on Multimedia Signal Processing* 47(4): 1423-1443.

During enrollment, the user presents a face image and fiduciary features are extracted from the image in the form of a vector X.[19] The feature vector is immediately converted into a codeword vector C using from an error correction code. The vector is mapped onto a random vector to be used as helper data during authentication. The helper data signal W is defined as the difference between the codeword vector and the feature vector, such that W x=C x-X. Figure 13 illustrates the algorithm during enrollment and authentication of the proposed helper data algorithm developed in a prior publication. During authentication the correct point is selected within a given radius ä.
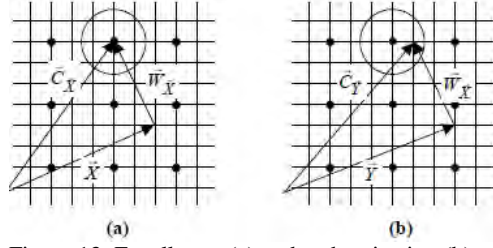
Figure 13: Enrollment (a) and authentication (b) procedures in the proposed helper data algorithm

Then the vector is quantized into a binary feature vector Q_i such that for each user i

$$Q_{i_t} = \begin{cases} 0 & \text{if} \quad (\vec{\mu}_i)_t \leq (\vec{\mu})_t \\ 1 & \text{if} \quad (\vec{\mu}_i)_t > (\vec{\mu})_t \end{cases}$$

Where ì ˉ is the mean of the enrollment feature vector, t is the component number, and (ì ˉ$_t$) is the mean of the

intraclass variability. Citing the unreliability of Q_i the researchers selected only the most reliable components from each vector resulting in Z_i. The vector is then ready to be protected. To achieve this they employed an error correction code with parameters (K,s,d) where K is the length of the codeword, s is the number of information

symbols, and d is the number of errors that can be corrected. First, a random binary sequence $S_{iD} \in \{0,1\}^s$ is

generated and encoded into a codeword C_i. Then the second helper data signal W2 is determined where

$$W2_i = C_i \oplus Z_i$$

The data (ì,$W1_{iD}$,$W2_{iD}$,h(S_{iD})) is saved to a storage device and will be referenced during authentication, where h(S_{iD}) is the hash value of the binary sequence S_{iD}. When the user attempts to authenticate, a vector of reliable features is extracted from the query face image. Template information (ì,$W1_{iD}$,$W2_{iD}$,h(S_{iD})) is pulled from the storage device. Both ì and $W1_{iD}$ are used to derive the binary feature vector Z'_{iD} which is necessary for determining the codeword C'_{iD} such that

$$C'_{iD} = Z'_{iD} \oplus W2_{iD} = Z'_{iD} \oplus (Z_{iD} \oplus C_{iD})$$

Decoding C'_{iD} leads to the recovery of the secret S'_{iD} and its hash value h(S_{iD}). Authentication is successful if this hash value matches that stored in the system.

Performance

The researchers tested the proposed method against one dataset with 237 faces and another with 96 faces. Respectively they achieved 35% FRR at 0% FAR meeting at 1.5% EER; and 3.5% FRR at 0% FAR meeting at 0.25% EER. The images that yielded more accurate results had smaller dimensions, fewer fiducial points, a smaller

---

[19] The researchers consider six such features in this publication: left and right eye, left and right eyebrow, mouth, and nose.

feature vector size, and less interclass variability. The security of the method might appear dubious compared to others because multiple data (ì,$W1_{iD}$,$W2_{iD}$,h(S_{iD})) are saved to the storage device. The researchers claimed that an attacker cannot retrieve a reliable feature vector Z_i even with knowledge of the helper data signal $W2_i$ and hashed secret h(S_i).

Zheng et al. (2006)

Zheng et al. proposed a method for producing highly entropic, noninvertible keys from iris images. They extended the fuzzy commitment scheme by Juels and Sudan (1999) by using K-nearest neighborhood classification. The lattice functions that map the biometric features onto lattice spaces are the only elements stored in the protected template. The researchers claimed that the original biometric cannot be recreated from the protected template even if the lattice functions are compromised.

Method

For each transaction, the user presents a biometric image from which a feature vector $x=(x_1,x_2...x_p)$ is extracted. The system generates an array of random binary strings sp stored as a codeword vector $c=(s_1,s_2...s_p)$. The codeword is treated as the coordinate x in the lattice space L(O,ä), where O is its origin and ä is its grid size. The origin O is defined as an array $O=(o_1,o_2...o_i)$ where each oi=xi-ä-2äs$_i$. The decoding function f() maps x to c using the lattice system L(O,ä). Each codeword element s_i is mapped onto a vector such that

$$s_i = \left[\frac{x_i - o_i}{2\delta}\right], i = 1, ..., p$$

The system then computes the secret key sk=h(c) or key pair (SK,PK)=K(c) and stores the lattice system L(O,ä). During authentication, the user presents a biometric image and attempts to unlock the codeword stored in the system. If successful, the codeword is used to compute the secret key or to seed K to derive (SK$_U$,PK$_U$). The codewords match where

$$c'_i = \begin{cases} c & \text{if} \quad ||x' - x_i|| \leq \delta \\ \text{not } c & \text{if} \quad ||x' - x_i|| > \delta \end{cases}$$

Performance

The researchers tested the proposed method against 150 iris images. They achieved ~2% EER where K = 7 and ~1.5% EER where the grid size ä=0.7, Error rates fell as the number of training samples rose.
The researchers noted that the security of the protected template depends on the hash function h(c) or the key generator K(c). They further note that the release of ä would leak trace amounts of information on the original biometric, even though only the lattice functions are stored in the template. The templates can be canceled by altering the value of the ä.

Uludag and Jain (2006)

Uludag and Jain proposed a variation of the fuzzy vault scheme by Juels and Sudan (2002) to protect fingerprint templates. A security concern in the original scheme was its tendency to leak trace amounts of information on the original biometric template, which theoretically could be used to reverse engineer the original template from the protected template. The goal of this study was to produce a more robust template protection method in which helper data leaks no sensitive information on the original biometric. The proposed method did not include error correction codes as the original fuzzy vault scheme did.

Method

During enrollment the user submits a fingerprint image from which a feature vector is extracted. Minutiae data are

quantized to account for intraclass variations. Concomitantly, a 128-bit secret string is randomly generated and a 16-bit cyclic redundancy check (CRC) is generated from the secret string. The CRC is appended to the secret string, forming a 144-bit string. This string can be represented as a polynomial p(u) with 9 coefficients with degree d=8 such that

$$p(u) = c_8 u^8 + c_7 u^7 + \cdots + c_1 u^1 + c_o$$

The bit string is used to create two sets of point pairs: a set of genuine points from the template and a set of chaff points randomly generated in the Galois field GF(2^{16}). The genuine set G and chaff set C are defined respectively as

$$G = [(u_1, p(y_1)), (u_2, p(y_2)), \ldots, (u_N, p(y_N))]$$

and

$$C = [(c_1, d_1), (c_2, d_2), \ldots, (c_N, d_M)]$$

where each u is a unique minutiae point in the original template, p(u) is the polynomial of u, N is the number of u; c and d are distinct sets of random, unique points, and M is the number of chaff points. Finally the genuine and chaff sets are combined as GUC and scrambled into the vault set V, such that

$$V = (v_1, w_1), (v_2, w_2), \ldots, (v_{N+M}, w_{N+M})$$

where v and w represent the scrambled points, N represents the number of minutiae templates, and M represents the number of chaff points. During authentication a user submits N query minutiae $Q=\{u_1^*, u_2^*, \ldots, u_N^*\}$ in an attempt to unlock vault V. Points u_N^* are compared with the abscissa values in V. Any vault point (v_t, w_t) that matches that in the input is recorded to a set to be verified in the decoding phase. The researchers construct the Lagrange interpolation of the polynomial to decode the vault set. From a given vault set $v=v_{N+M}, w_{N+M}$ the corresponding polynomial is

$$p^*(u) = \frac{(u - v_2)(u - v_3) \ldots (u - v_{D+1})}{(v_1 - v_2)(v_1 - v_3) \ldots (v_1 - v_{D+1})} w_1 + \cdots + \frac{(u - v_1)(u - v_2) \ldots (u - v_D)}{(v_{D+1} - v_1)(v_{D+1} - v_2) \ldots (v_{D+1} - v_D)} w_{D+1}$$

which when calculated in Galois field GF(2^{16}) is expressed as

$$p^*(u) = c_8^* u^8 + c_7^* u^7 + \cdots + c_1^* u^1 + c_0^*$$

If at least D + 1 query minutiae points match a genuine minutiae point in the vault set, the correct secret S will be decoded and the user is authenticated.

Performance

Uludag and Jain tested the proposed method against 800 fingerprint images using automatic alignment. They mixed 24 genuine minutiae points with 200 chaff points per vault. The results from two trials showed 27.4% FRR and 15.5% FRR[20] respectively at 0% FAR. They claimed that the false rejections were due to errors in helper data or poor quality input images. Their implementation of the iterative closest point algorithm aligned input features to template features, something that other researchers at the time had neglected to consider.

Freire-Santos et al. (2006)

Freire-Santos et al. proposed a variant of the fuzzy vault scheme by Juels and Sudan (2002). Prior to their research,

---

[20] FRR calculated from reported GAR.

template protection methods based on the fuzzy vault scheme required manual prealignment of the input images. Freire-Santos attempted to align the input images w2automatically. Their methodology follows that of Uludag and Jain (2006).

Method

As shown in Figure 14, during enrollment, the user writes a signature from which a template feature vector T is extracted in the form of N 16-bit units. A checksum of S is appended to S. A polynomial $p(x)$ is then constructed with degree $D=K/16$, such that

$$p(x) = S_1 x^n + \ldots + S_D x^1 + S_{D+1}$$

Polynomials are projected for all points in the feature vector, forming genuine set G, such that

$$G = \{t_1, p(t_1), \ldots, (t_N, p(t_N))\}$$

A chaff set C with M points is also generated where $d_i \neq p(c_i)$ such that

$$C = \{c_1, d_1, \ldots, c_M, d_M\}$$

The genuine and chaff point sets $G \cup C$ are scrambled into the vault set V such that

$$V = \{(v_1, w_1), \ldots, (v_{N+M}, w_{N+M})\}$$

The vault, then, is nothing more than a disordered union of the genuine and chaff point sets. That the two sets are arranged in a random fashion makes it nearly impossible to distinguish genuine and chaff points. Only by knowing $D + 1$ or more genuine points can a polynomial be reconstructed to distinguish the genuine points.
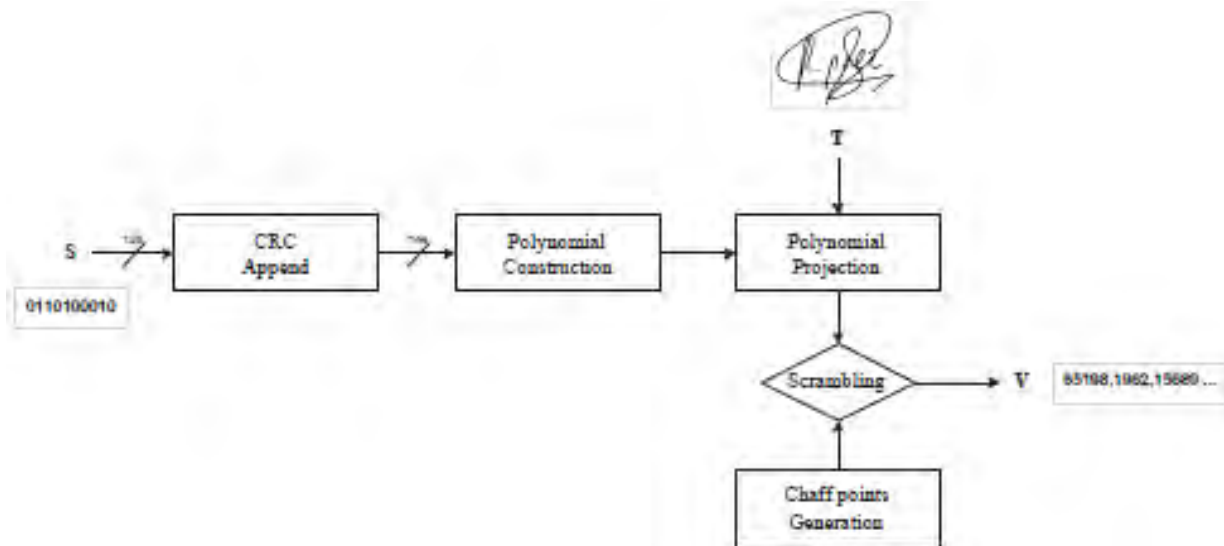
Figure 14: Encoding process (2006: 3)

During authentication, the user presents a signature from which a template feature vector Q is extracted. To unlock the vault, the values of the feature vector from an input image are compared against those in the vault. Specifically if any point q1 is present in the abscissa values of the vault set, then the point will be used as a candidate to reconstruct the secret polynomial. The secret polynomial is interpolated with all combinations of the point candidates using the

Lagrange method, also used by Uludag and Jain (2006). If the division between this new polynomial and the stored polynomial is equal to zero, then the secret is valid with an error probability of 2^{-16}; otherwise it is invalid.

In their implementation, Freire-Santos et al. preprocessed handwritten signatures by omitting the first and last 10% of the images, normalizing the shapes based on the center of mass and the standard deviations of the function values, and smoothing the images to reduce noise-related errors. They constructed their vaults using the maxima and minima, in the same fashion that Uludag and Jain (2006) used the coordinates of fingerprint minutiae.

Performance

The researchers tested their method against 16,500 handwritten signatures. After 15,625 imposter comparisons, they achieved 57.30% FRR at 1.18% FAR and 0.32% FAR for skilled and random forgeries, respectively. These results are far from ideal, but it should be noted that the signature modality typically yields less accurate verification rates than fingerprint, iris, or face biometrics. Further testing on more reliable biometric modalities and with error correction strategies might yield lower error rates.

Sutcu et al. (2007)

Sutcu et al. critiqued the practical application of existing fuzzy cryptosystems, arguing that a lot of entropy would be lost when generating keys from quantized templates. They described a cryptosystem that they developed in a previous work[21] and applied it to an authentication scheme using face biometrics. The proposed method is similar to the fuzzy vault scheme proposed by Juels and Sudan (2002).

Method

During enrollment, the user i presents a biometric image from which a feature vector $V_i = [v_{i1} \; v_{i1} \ldots v_{in}]^T$ of size n is extracted several times to train the system. Each midpoint v_{ij} and range size δ_{ij} of the feature vectors is estimated from the training set. The global range sizes $MN_j = \min_t(mn_{ij})$ and $MX_j = \max_t(mx_{ij})$ are quantized into a codebook C_j such that

$$C_j = \{MN_j - r_j, MN_j - r_j + \delta_j, MN_j - r_j + 2\delta_j, \ldots, MN_j - r_j + L_j\delta_j\}$$

where r_j is a random positive number and L_j is an integer that satisfies $MN_j - r_j + L_j\delta_j \geq MX_j$. This allows the data to be mapped onto a discrete domain, which was a requirement of the fuzzy vault scheme by Juels and Sudan (2002). Then a vault set P_i is derived from the codebook as a vector expressed as

$$P_i = [p_{i1} \; p_{i2} \ldots p_{ik}]^T$$

where each p is defined as

$$p_{ij} = Q_j^i(\bar{v}_{ij} - \bar{v}_{ij})$$

and where $Q_j^i(\bar{v}_{ij})$ is the codeword in C_j^i that is closest to $(\bar{v}_{ij})$. Reconstruction of the original biometric is successful if

$$-d_{ij} \leq Q_j^i(\bar{v}_{ij}) < d_{ij}(x+a)^n = \sum_{k=0}^{n} \binom{n}{k} x^k a^{n-k}$$

---

[21] Qiming Li, Yagiz Sutcu and Nasir Memon, 2006, "Secure Sketch for Biometric Templates," in *Lecture Notes in Computer Science* 4284(2006): 99-113.

where the discrete range size $d_{ij}=\lceil \delta_{ij}/\delta_j \rceil$ is the user specific error tolerance bound for the jth component and the

quantization step δ_j is defined as $\delta_j = \alpha \min(\delta_{ij})$; α is a parameter between 0 and 1. During authentication, feature vectors from an input image are extracted, trained, and quantized in the same fashion as the enrollment process. If the dataset matches that of one stored in the dataset, authentication is deemed successful.

Performance

The researchers tested the proposed method against face images. After 1,216 genuine and 183,616 imposter authentication attempts, they achieved ~3.8% FRR at ~0.7% FAR where α was a recommended value of 1. Its performance can be linked to the proposed quantization method, which is what distinguishes this method from other fuzzy cryptosystems.

<u>Nandakumar et al. (2007)</u>

Nandakumar et al. wrote this article in reaction to growing concerns about the security vulnerabilities in the fuzzy cryptosystems, namely that the vault sets could not be cancelled and were susceptible to collusion attacks. They attempted to produce cancelable vault sets for fingerprints by integrating passwords to the general method of the fuzzy cryptosystem. The method is similar to that proposed by Teoh et al. (2004) in that it authenticates a user based on who they are and what they have.

Method

During enrollment the user presents a password and a fingerprint image from which a feature vector (x,y,è) is extracted, where (x,y) are the minutiae coordinates and è is the angle of each minutiae point. The minutiae points are classified according to their location in each quadrant of the image. Then the password is split into four equally sized units, [22] which are then distributed evenly among the quadrants. Each password unit is divided into three components T_x, T_y, and $T_è$. T_x and T_y represent the amount by which the minutiae will be translated, and $T_è$ represents the degree to which they will be rotated. The new minutiae attributes Q'_x, Q'_y, , and $Q'_è$, are derived from the addition of the translations values and the original values modulo the appropriate range, such that

$$Q'_x = (Q_x + T_x)\operatorname{mod}(2^{B_x})$$
$$Q'_y = (Q_y + T_y)\operatorname{mod}(2^{B_y})$$
$$Q'_\theta = (Q_\theta + T_\theta)\operatorname{mod}(2^{B_\theta})$$

Observe that a change in the password would affect the values of Q_x', Q_y', and $Q_è'$. Thus if the user were to change his or her password, the template would be cancelled. Next, the minutiae points are encrypted in the vault set. To construct the vault, the researchers use Lagrange interpolation and cyclic redundancy checks instead of the conventionally used Reed-Solomon polynomial reconstruction. Each minutiae point, represented as an element in the Galois field $GF(2^{16})$, is quantized into binary strings Q_x, Q_y, and $Q_è$. These minutiae points form a genuine set. A large set of chaff points is combined and shuffled with the genuine set to form the vault set.

During authentication, the user presents a password and a query fingerprint image. Minutiae from the query image are transformed by the password using the same process as during enrollment. Helper data from the vault set and query set are aligned with the transformed query template using a trimmed iterative closest point algorithm. [23] This singles out many of the chaff points from the vault set, assuming the query fingerprint is indeed the same as the enrolled fingerprint. The researchers claimed that the helper data leaks no information on the original biometric, which, if valid, poses no significant security threat.

---

[22] The researchers assumed the password length to be 16-bits, or 8 characters, which perfectly aligned with the number of minutiae points. How to handle a variable-length password is a major concern for the usability this method.
[23] The researchers cite D. Chetverikov et al., 2002, "The Trimmed Iterative Closest Point Algorithm," in *Proceedings of the international Conference on Pattern Recognition*: 545-548.

Performance

The researchers tested their approach against two datasets with 800 and 640 fingerprint images. Respectively the results yielded 10-19% FRR and 19.4-26.2% FFR[24] at 0% FAR with 58-70 bits of security including the password. FRR increased as the size of the polynomial increased. Additionally, they found the vault sets to be more uniformly distributed than the original template, fortifying them against attacks. What this approach gains in security it loses in usability. While its results showed that it can reliably protect against unauthorized access, it may reject too many genuine users to be considered acceptable. This may have been the only attempt at combining fuzzy cryptosystems with multifactor authentication, and the results do not bode well for their interplay.

Nandakumar and Jain (2008)

Nandakumar and Jain applied fuzzy cryptosystems to multimodal templates that combined fingerprint minutiae and IrisCodes. The proposed method transformed both feature sets into a common format and fused them into a single vault set following the fuzzy vault scheme proposed by Juels and Sudan (2002). The setup of the method mirrored that proposed by Nandakumar et al. (2007) in that biometric features were represented in Galois field $GF(2^{16})$, the key size was set to 16n bits where n was the degree of polynomial P, and error correction was achieved through Lagrange interpolation and CRC instead of Reed-Solomon codes.

Method

For each transaction the user presents a fingerprint and an iris. Features from fingerprint and iris images were segmented and converted to a common format. Upon presenting a fingerprint, the coordinates and angles of the highest quality minutiae points were extracted, quantized, and concatenated into a 16-bit number. [25] A set of high curvature points was also extracted and stored in the vault to aid the alignment of the stored template with the query templates. Upon presenting an iris, the IrisCode template is extracted and transformed by a random salt. To perform the transform, and IrisCode IT is split into r distinct components $[I_T^1 ... I_T^r]$. Then r random binary vectors $K^1...K^r$ are generated. A BCH encoder is applied to each binary vector $K^1...K^r$ resulting in the codewords $H(K^1)...H(K^r)$. The codewords were XORed with the transformed IrisCode components $[I_*^1 ... I_*^r]$ such that any given component $I_*^i = I_T^i \oplus H(K^i)$. Thus the transformed IrisCode I_* can be expressed more simply as

$$I_* = F_1(I_T, K_1)$$

where F_1 is the salting function that transforms the I_T based on K_1.

Nandakumar and Jain considered the proposed on three applications of multiple biometrics: (1) where the template consisted of multiple impressions of the same fingerprint; (2) where the template consisted of multiple fingerprints; and (3) where the template consisted of multiple modalities, particularly fingerprint and iris. In the case where multiple fingerprint impressions were to be stored as a single template, they used a "mosaicing" technique. [26] In the case where multiple fingerprints are to be stored, the union of all the minutiae sets $[M_B^T_1 ... M_B^T_r]$ formed the basis of the vault. In the case where fingerprint and iris features were to be stored, the vault set was derived from the union of all points between the two feature sets where Hamming distance HD ≥ 2.

Performance

The researchers tested the proposed method using multiple fingerprint templates and multimodal templates. The experiment on multiple fingerprint templates achieved 10% FRR[27] at 0.02% FAR and 2.5% FTCR. The experiment

---

[24] FRR calculated from reported GAR.
[25] The means by which the minutiae points were processed resembled that by Nandakumar et al. (2007).
[26] The mosaicing technique was adapted from A. Ross, S. Shah, and J. Shah, "Image Versus Feature Mosaicing: A Case Study in Fingerprints," in P*roceedings of SPIE Conference on Biometric Technology for Human Identification* (6202), (2006): 1–12.
[27] Calculated from 90% GAR.

on fingerprint and iris images achieved 1.8% FRR[28] at 0% FAR and 0% FTCR, and it produced a vault key size of 224 bits. Feasibly the multimodal test could meet the performance target of 1% FRR at 0% FAR with some tuning. These results suggest that multimodal authentication is superior to multifactor authentication as a means of augmenting security and performance in fuzzy cryptosystems.

Ŏrencik et al. (2008)

Ŏrencik et al. proposed a variation of the fuzzy vault scheme by Juels and Sudan (2002) that was designed to resist brute force attacks. The researchers observed that genuine points could be distinguished from chaff points based on the distances between them in conventional vault sets. The proposed method entailed a more sophisticated means of distributing chaff points and required storage of multiple chaff polynomials, a novel contribution to the fuzzy cryptosystem.

Method

The researchers generated chaff points such that each one was at least t Euclidian distance units apart from a genuine point and at least t' Euclidian distance units apart from any other chaff point. The threshold t is set according to the distribution of the genuine points, but the researchers did not formalize a method for selecting this threshold. Figure 15 compares the distribution of chaff points in the original fuzzy vault scheme by Juels and Sudan (2002) and the proposed method, where t = 18 and t '= 8. The chaff point distribution of the proposed method more closely resembles that of the genuine points, such that an attacker cannot easily distinguish the genuine points from chaff points.
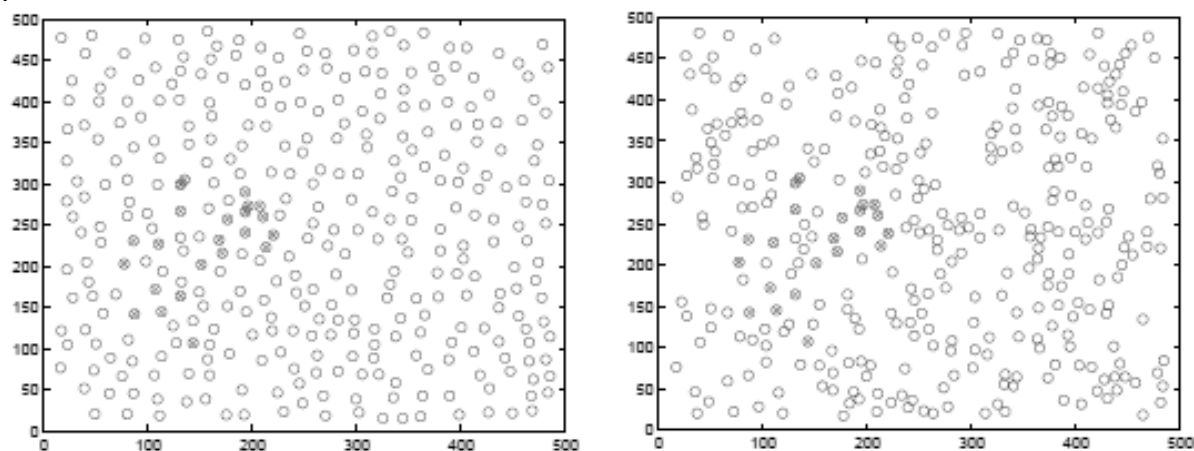
Figure 15: Chaff point distribution by Juels and Sudan (2002) (L) and Ŏrencik et al. (2008) (R); genuine points darkened (2008: 40).

To construct the chaff polynomials, first generate a random number r that is close to the number of genuine points n. For the first polynomial elect k-1 random points from the vault set and one random point from a pool of random chaff points. For the other polynomials select k random points from the vault set, find the polynomial of degree k-1 that passes through the selected points, and add the polynomial to a list of chaff polynomials. Verify if there are any other points in the vault set laying on the polynomial. Decrease r by the number of points in this polynomial. Select r points from the pool of chaff points and evaluate them on the chaff polynomial. Place the resulting values in the vault set. Repeat this process until pool of chaff points is empty.

Performance

The researchers tested the proposed method against 360 fingerprint images under two attack scenarios: brute force attacks and Reed Solomon decoding. They achieved 1.5% FRR at 0% FAR where the vault size was 300, the threshold t=18, k=10, n=15 on average, and the minimum distance between chaff points was 8. These are decent results compared to other variations of the fuzzy cryptosystem reviewed in this report. They found that it was faster

---

[28] Calculated from 98.2% GAR.

to recover the secret polynomial from the vault set using Reed Solomon decoding when the number of chaff points was large. The researchers were able to hide 30 chaff polynomials in the vault set using the proposed method. They claimed that this decreased the probability of recovering the secret polynomial by brute force from 100% to 3.3%.

Nagar et al. (2009)

Nagar et al. found that empirical tests on fuzzy cryptosystems yielded poorer results than other methods because they were optimized to work with limited fingerprint information. The researchers proposed a variation of the method that stored minutiae descriptors in the vault sets, providing more detailed information on a fingerprint than just the coordinates of its minutiae points including the frequency and orientation of the ridges around each minutiae point. The protected template was a nested vault set, in which the abscissa values of the minutiae points were stored in one vault set and the ordinate values were stored in a another vault set.

Method

During enrollment a 16-bit cyclic redundancy check code is appended to a 16n-bit key K and divided into (n+1) blocks of 16 bits each. The blocks served as the coefficients of a secret polynomial p(x) of degree n represented in Galois field GF(2^{16}). Minutiae points are selected from the template based on their quality and separation from one another, as done by Nandakumar et al. (2007) The coordinates and angles of the quality minutiae points, along with a large number of randomly generated chaff points, are stored in the vault set V.

The researchers used minutiae descriptors to encrypt the ordinate values[29] of the minutiae points. [30] The ordinate value for each minutiae point was used to obtain a codeword C from an error correction code. The design of the proposed method requires that the minutiae descriptors be represented in binary format. The binarization process consists of four stages: (1) estimating the missing values based on nearest neighbors; (2) reducing the dimensionality of the descriptor; (3) encoding Gray codes; and (4) selecting the discriminable bits. The secure ordinate value $C_i = (D_i^b \oplus C_i)$, along with the abscissa values, are stored in the dataset as helper data. Descriptors for the chaff points are randomly chosen from the set of all descriptors in the dataset. One might consider this to be a vulnerability whereby an attacker could analyze the occurrence of chaff point descriptors to distinguish genuine points from chaff points. Such an attack would seem especially plausible on a small scale dataset where the diversity of the minutiae descriptors is limited.

During authentication, the user presents a fingerprint image which is aligned with one or more templates using high curvature points as described in Nandakumar et al. (2007). The quality minutiae points are selected from the query fingerprint and matched with points in the vault set in order to filter out most of the chaff points. Minutiae descriptors are extracted from the fingerprint and binarized. The descriptor is XORed with each selected query minutiae and its ordinate value to obtain a codeword C', which is decoded to obtains a representation of the ordinate value. If the ordinate value is correctly decoded for (n+1) genuine points in the vault, the polynomial p(x) is correctly reconstructed and the query is validated.

Performance

The researchers tested the proposed method against 100 fingerprint images from the FVC2002 DB2 dataset, conducting 100 genuine comparisons and 9900 imposter comparisons. Results yielded 5% FRR at 0.01% FAR where the polynomial degree n=6. FRR rose abruptly where the polynomial degree n≥9. They also tested the method using principal components analysis to reduce the dimensionality of the descriptors. This scenario yielded higher false acceptance rates than when principal components analysis was not used.

Álvarez et al. (2009)

Álvarez et al. were among the few researchers to implement the fuzzy extractor method proposed by Dodis et al.

---

[29] In a coordinate (x, y), y represents the ordinate.
[30] The researchers adopt the methodology proposed by J. Feng, 2008, "Combining Minutiae Descriptors for Fingerprint Matching," in *Pattern Recognition* 41(1): 342-352.

(2008). The proposed method is resistant to collusion attacks because the biometric input is not used in the creation of the polynomial; instead the coordinates of the minutiae points are salted by a secret key that is unique across applications and can be reissued in the event that the template is compromised.

Method

During enrollment, the user presents an iris image and a predefined secret key S represented in a given base.[31] Helper data from the iris image is stored in the dataset. The coefficients of the polynomial $p(x)$ of degree d are derived from bits of the secret key $S = \{s_0, s_1 \dots, s_D\}$ such that

$$p(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_d x^d$$

Then n random points are computed such that $y_i = p(x_i), 0 \leq i \leq n-1$ where n is a parameter that controls the tolerance of the templates. The value of n should be much greater than d. Reed-Solomon encoding concatenates the coordinates (x_i, y_i) of the n points forming a codeword set $C = \{c_0, c_1, \dots, c_{n-1}\}$. A hash function $h(\cdot)$ obfuscates the codeword set C producing a set of hash values

$$H = [h(c_0), h(c_1), \dots, h(c_{n-1})]$$

Then the iris template B is divided into n parts $B = b_i 0 \, \| b_i 1 \| \dots \| b_i(n-1)$. Each value $b_i, 0 \leq i \leq n-1$ is subtracted from each codeword of the set C, producing in the delta set Δ in which each element $\delta_i = c_i - b_i, 0 \leq i \leq n-1$ such that

$$\Delta = \{\delta_0, \delta_1, \dots, \delta_{n-1}\}$$

Stored in the dataset are the hash set H, the delta set Δ, and control parameters necessary for authentication, which include: the polynomial degree d, the Reed-Solomon parameters (k, nRS, m), the hash function used, and the base in which S is represented.

During authentication, the user presents a query iris image and secret key. The query template $\overline{B}$ is divided into n parts such that $\overline{B} = b_i 0 \, \| b_i 1 \| \dots \| b_i (n-1)$. The elements of $\overline{B}$ and the stored delta set Δ are used to compute the codeword set $\overline{C} = \{\overline{c}_0, \overline{c}_1, \dots, \overline{c}_{n-1}\}$. The elements of $\overline{C}$ are hashed using the stored hash function, and the hashed elements of $\overline{H}$ are compared against those stored in the dataset. If at least $d + 1$ values coincide, the template is considered a match. But the secret key also must be verified before authenticating the user. A Reed-Solomon decoding algorithm obtains at least $d + 1$ points (x_i, y_i). Lagrange interpolation obtains the coefficients of the secret polynomial $p(x)$. If the polynomial is successfully reconstructed, the secret S would be revealed and the user would be authenticated.

Performance

The researchers tested the proposed method against 175 iris images using an algorithm they developed in Java. They achieved 11.1% FRR at 0.67% FAR, where the base of S is 512, the polynomial degree $d = 21$, and $n = 312$. These results are not acceptable for most practical applications, and they are particularly unsatisfactory given that iris applications typically yield lower error rates. But the fuzzy extractor method has been observed little in practice, and the method ought to endure more rigorous experimentation using various combinations of parameters and inputs.

<u>**Merkle et al. (2010)**</u>

---

[31] Base 10, 16, 256, 512, etc.

Merkle et al. published this paper in reaction to the concern that variations of the fuzzy vault scheme produced templates with no more than 50 bits of entropy when applied to fingerprint biometrics.[32] The researchers pursued the suggestion of those who made that claim, which was to buttress the fuzzy fingerprint vault method using multiple fingerprints. The proposed method naturally follows that of Nandakumar and Jain (2008) who also applied the fuzzy vault scheme to encrypt singular representations of multiple fingerprint impressions.

Method

Upon presenting a fingerprint image, features are extracted in the form of a vector (θ_1, a_1, b_1) which respectively indicates the minutiae coordinates and the index of the fingerprint from which the minutiae point originated. The researchers claimed it would be too taxing for the system to distinguish genuine points from chaff points were the vector to include information on the minutiae angles; therefore they did not store angle data in the vector. The researchers optimized feature extraction in several ways. One novel optimization was to restrict the selection of genuine and chaff points to those within a confined area.[33] Optimizations developed from prior studies include the exclusion of unreliable minutiae for the feature vector during enrollment, the enforcement of a minimum distance between genuine and chaff points, and the enforcement of a minimum number of minutiae points per finger.[34] And they pre-aligned the fingerprints and the threshold for rotation. The feature vectors of all fingerprints captured by the acquisition device were stored in the same set rather than in separate sets. Doing so exponentially increased its resistance to brute force attacks.[35] However the researchers observed that the proposed method might be vulnerable to brute force attacks than other variants of the fuzzy cryptosystem because an attacker can verify when a polynomial is recovered using the hashed value of the secret coefficients, thereby enhancing the efficiency of an attack. Unlike the original fuzzy vault scheme by Juels and Sudan (2002), the proposed method evaluated the secret polynomial according to the minutiae indexes rather than the actual biometric data.[36]

During authentication, the user submits a query fingerprint image. The image is prealigned and a vector of quality minutiae points is extracted from the aligned image. The feature vector is matched against one or more templates in the dataset. A Reed-Solomon decoder, specifically the Peterson-Berlekamp-Massey decoder used by Juels and Sudan (2002), is used to recover the secret polynomial, which will be recovered only if there are at least $(w + k)/2$ matching points between the query template and the genuine points in the vault set. The correctness of the polynomial is compared against the hash value of the true polynomial stored in the dataset.

Performance[37]

Merkle et al. tested the proposed method against 864 fingerprints. They tested a control group without any chaff points, and the results were optimal at 89% FRR where $\delta_v = 7$. Using this as a benchmark, they increased the minutiae quality value Q over several iterations. Where $Q = 0.1$ the false and genuine match rates remained nearly unchanged, but where $Q = 0.2$ the false match rate rose by 30%. Therefore the most practical results offered by the proposed method are approximately 1% FRR where $\delta_v = 7$ and $Q = 0.1$. Enforcing a minimum number of minutiae per finger increased match rate by up to 3% and reduced enrollment rate by up to 7%, with at least 9 minutiae per finger being the optimal. Their prealignment method omitted all poor quality fingerprints at the expense of 20% false positives, whereas without prealignment omitted 86% poor quality images at the expense of 35% false positives. As the value of the tolerance parameter rose, false match rates rose significantly while false non-match rates bore no significant change.

4.4   Homomorphic Encryption

---

[32] See P. Mihailescu, A. Munk and B. Tams, 2009, "The Fuzzy Vaults for Fingerprints is Vulnerable to Brute Force Attack," in *BIOSIG 2009: Biometrics and Electronic Signatures*: 43-54.

[33] Such that an area $M := \{(\theta, a, b) \mid \theta \leq f^{\top}(a, b) \, E\}$. This was found to be the most commonly plotted area from a sample of 5.8 million minutiae points. See p. 3.

[34] See pp. 4-5 for more information on quality filtering optimizations.

[35] To store each feature vector in its own set and concatenate the sets would result only in a linear increase of entropy. An exponential increase is significant.

[36] See pp. 5-6 for more information on encoding the secret polynomial including pseudocode for the enrollment stage.

[37] Based on their empirical results, the researchers offer a list of recommended parameter values on p. 11.

An encryption method is homomorphic if the structure of the ciphertext is preserved in the encryption of the plaintext. Homomorphism has a "malleable" property, meaning that the ciphertext can be converted into another ciphertext that also reverts to the original plaintext. Homomorphic encryption can be used to calculate the similarity between an input templates and stored templates in the encrypted domain, preventing servers from extracting sensitive information from a query. Many of the proposed homomorphic encryption methods make use of existing cryptosystems proposed by Paillier, Goldwasser-Micali, and ElGamal, all of which are semantically secure protocols. Homomorphic encryption may be applied to one step in the template protection processes. This section of the report reviews methods in which homomorphic encryption protocols are the primary means for protecting biometric templates.

4.4.1   Method

Paillier

Variations of the Paillier cryptosystem are additively homomorphic, meaning that the ciphertext is equal to the sum of two plaintexts (x_1, x_2) such that

$$å(x_1) \cdot å(x_2) = å(x_1, x_2 \bmod m)$$

The encryption of a plaintext x is expressed

$$å(x) = g^x r^m \bmod m^2$$

where m is the modulus g with a block size r.

Goldwasser-Micali

Variations of the Goldwasser-Micali cryptosystem are multiplicatively homomorphic, meaning that the ciphertext is equal to the product of two bits (b_1, b_2) such that

$$\varepsilon(b_1) \cdot \varepsilon(b_2) = \varepsilon(b_1 \oplus b_2)$$

ElGamal

Variations of the ElGamal cryptosystem are multiplicatively homomorphic, meaning that the ciphertext is equal to the product of two plaintexts (x_1, x_2) such that

$$\varepsilon(x_1) \cdot \varepsilon(x_2) = \varepsilon(x_1 \cdot x_2)$$

4.4.2   Vulnerabilities

The malleable property of homomorphic encryption allows someone with access to a ciphertext to modify its contents and produce a new plaintext. Theoretically this would allow an attacker with access to a dataset of secured templates to modify the contents such that it would resemble the attacker instead of the genuine owner.

Nagar et al. (2006) suggested the application of a homomorphism to obfuscate the helper data used to unlock vault sets in fuzzy cryptosystems.[38]

4.4.3   Performance

There have been few empirical tests on template protection methods using homomorphic encryption. But verification rates are impressive in the few tests that have been conducted. Ye et al. (2009) achieved the best results

---

[38] See Nagar, Abhishek, Karthik Nandakumar and A. K. Jain, "Biometric Template Security," *SPIE*: 3.

using homomorphic encryption but did not meet the performance target of 1% FRR at 0.1% FAR. The protected templates matched or exceeded the minimum length necessary for use as cryptographic keys in common security protocols like AES. Barni et al. (2010) proposed a method that was able to identify an 80-bit template from a dataset of 100 templates in 45.58 seconds. Huang et al. (2011) proposed a method that improved that speed by almost five times.

4.4.4   Articles

Barbosa et al. (2008)

Barbosa et al. proposed a parametric key generation method that borrowed the encryption and decryption algorithms from the Paillier cryptosystem.[39] The researchers adapted the work of Bringer et al.[40] to develop a set of identification classifiers. The proposed method does not expose identities in the process of authentication or identification, upholding the privacy of the user in distributed authentication systems like those on the Internet. They claimed their method delivered more accurate results even among behavioral modalities. They criticized fuzzy cryptosystems and other methods based on error correction codes for their poor performance and their ability to secure data against anything except eavesdropping attacks. The researchers did not test their method empirically.

Method

The proposed method assumes that the acquisition device is capable of processing the biometric image into a binary string and performing cryptographic operations on the string. The system initializes by generating a secret key using the key generation algorithm from the Paillier cryptosystem. Given a security parameter 1^k the algorithm generates the following: n=pq where p and q are two large random prime numbers; $\lambda = \text{lcm}(p - 1, q - 1)$; and a random integer $g \in \mathbb{Z}_{n^2}^*$. It follows that the multiplicative inverse μ exists, such that

$$\mu = \left(L\left(g^\lambda \bmod n^2 \right) \right)^{-1} \bmod n$$

hence the public key k_e=(n,g) and the secret key k_d=(μ,λ). For each transaction the user submits a query from which biometric features are extracted in the form of a vector v=($v_1\ldots v_k$). The features are classified according to the public parameters and the profile information, returning a set of classification values. The classification algorithm, a "support vector machine,"[41] uses homomorphic encryption to compute the classification values, such that

$$c_j = \prod_{i=1}^{s} K\left(\text{auth}, SV_{i,j}\right)^{\alpha_{i,j}r_j} = E_{\text{Paillier}}\left(\sum_{i=1}^{s} \alpha_{i,j} K\left(v, SV_{i,j}\right), \text{params}\right)$$

where $SV_{i,j}$ contain vectors that define the inner and outer hyperplane in a k-dimensional feature space, and K is a function that projects data onto a higher dimensional space and computes the scalar product. The encryption algorithm produces a ciphertext c=$g^m \cdot r^n \bmod n^2$ where m is a plaintext message, r is a random integer, and n and g are derived from the public key k_e=(n,g). The ciphertext is shuffled into a random vector to be stored in the dataset. During authentication, the system decrypts the elements of the shuffled ciphertext. The decryption algorithm outputs a plaintext m=L(cλ mod n^2)·μ mod n where μ and λ are derived from the secret key k_d=(μ,λ).

Ye et al. (2009)

Ye et al. designed a biometric authentication protocol that preserved the anonymity of the authenticating user. They pursued three goals. Firstly, they sought to build a system that never revealed the identity of the user to the system.

---

[39] See Pascal Paillier, 1999, "Public-Key Cryptosystem Based on Composite Degree Residuosity Classes," in *Lecture Notes in Computer Science* 1592: 223-238.

[40] Bringer, J. et al., 2007, "An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication," in *Lecture Notes in Computer Science* 4586: 96-106.

[41] See K. Crammer and Y. Singer, 2001, "On the Algorithmic Implementation of Multiclass Kernel-Based Vector Machines," in *Journal of Machine Learning Research* 2: 265-292.

Methods in prior research often encrypted the templates after each transaction but exposed the owner of the template at some point in the transaction process. Secondly, like prior researchers, they sought to build a system that withstood intraclass variability. And thirdly, they sought to construct a scalable system that would perform well in environments with large datasets, while controlling the tradeoff between security and performance. Their solution to the complexity issue was to keep an authenticating user anonymous only to k but not the entire dataset, where k is a parameter of anonymity. The proposed method was similar to the k-anonymity model by Sweeny. [42] The proposed method optimized the dissimilarity among members of the same k-member cluster. The researchers mentioned the possibility of designing a template protection method based on secure multiparty computation, but they opted for homomorphic encryption due to its allegedly superior efficiency.

Method

The proposed system consists of three devices: a server, a dataset, and a biometric acquisition device. These devices are used in three high level procedures. In the first procedure, triggered by an enrollment request, the server preprocesses the image by way of k-Anonymous Quantization. The resulting quantization table will be used to narrow the scope of future queries from the entire dataset to a group of likely candidates called a "k-member cluster," which was designed to boost the speed of identification. The server stores the quantization table in a publicly available dataset. In the second procedure, triggered by an authentication request, indexes from the dataset are selected in a secure fashion. In the final procedure, distance measurements between a query template and one or more protected templates are conducted in the encrypted domain.

During enrollment the user presents an iris image x. The researchers use the Paillier homomorphic encryption scheme to derive the public key from the input x such that

$$Enc_{pk}(x) = [(1 + N)x \cdot r^N \bmod N^2]$$

where N is the product of two secret primes and r is a random number.

During authentication, the user submits a public key and an iris image. A modified Hamming distance algorithm measures the dissimilarity between the query iris pattern and one or more stored iris patterns in the encrypted domain. [43] The distance between the query iris and one or more secure templates is calculated in the encrypted domain.

Performance[44]

The researchers tested the proposed access control system against 1,948 iris images from the CASIA dataset. It took 11.5 hours to encrypt and match 10,000 iris images, or about 4.15 seconds per image, from the dataset on a machine with a 2.4 GHz CPU and 2 GB RAM. They achieved ~4% FRR ~0% FAR.

Rane et al. (2009)

Rane et al. designed a homomorphic cryptosystem for securing fingerprint templates and computing the Hamming distance or Euclidian distance between templates in the encrypted domain. The researchers adopted the Paillier encryption protocol. They did not test the accuracy of the proposed method.
Method

For each transaction, the user presents a fingerprint from which a binary feature vector x^n is extracted. The query will be compared against a protected template y^n stored on the dataset. The researchers adopted the Paillier cryptosystem is used to encrypt and decrypt the template information prior to computing the distance metrics, such that

---

[42] See L. Sweeny, "*k*-Anonymity: A Model for Protecting Privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(50), 557-570, 2002.
[43] See p. 4 for a description of their modification.
[44] Results are discussed in great detail on pp. 12-15.

$$\xi_r(m) = g^m \cdot r^N \mathrm{mod}(N^2)$$

where r is a randomly generated number, p and q are large prime numbers, N=p·q, and g is a number selected such that gcd(L(g$^{\ddot{e}}$ mod (N²))N)=1. A public key is defined as (N,g) and a private key is defined as (p,q). The client encrypts the query fingerprint x_i into $\hat{i}_{r_i}(x_i)$ using the above protocol. The encrypted results are transferred to the server. The server then computes the following:

$$\bar{y_i} = -2y_i \,\mathrm{mod}(N)$$

$$\xi_{r_i}(-2x_iy_i) \equiv \lfloor \xi_{r_i}(x_i) \rfloor^{\bar{y_i}} \mathrm{mod}(N^2)$$

$$\xi_{r_c}(C) \equiv \xi_{r_c}\left(-\sum_{i=1}^{n} 2x_iy_i\right) \equiv \prod_{i=1}^{n} \xi_{r_i}(-2x_iy_i)\,\mathrm{mod}(N^2)$$

where $C = -\sum_{i=1}^{n} 2x_iy_i$ and $r_0 = \prod_{i=1}^{n} r_i \,\mathrm{mod}(N)$. The result $\xi_{r_0}(C)$ is . This computation is executed in the encrypted domain, so the server has no knowledge of C or r_c . The server then generates a random number r_b and computes

$$\hat{i}_{rd}(B{+}C) \equiv \hat{i}_{rb}(B)\,\hat{i}_{rc}(C)\,\mathrm{mod}(N^2)$$

where $r_d = r_b\, r_c \,\mathrm{mod}(N)$. The results are transferred to the client. The client then generates a random number ra and computes

$$\xi_r\big(d(x^n, y^n)\big) = \xi_r(A + B + C) \equiv \xi_{r_a}(A)\xi_{r_d}(B + C)\,\mathrm{mod}(N^2)$$

where $d(\cdot)$ is the binary Hamming distance, $r = r_a r_d \,\mathrm{mod}(N)$, $A = \sum_{i=1}^{n} x_i$ and $B = \sum_{i=1}^{n} y_i$. That value of r is unknown to Alice. The squared Euclidian distance can be expressed as

$$d(x^n, y^n) = \sum_{i=1}^{n}(x_i - y_i)^2 = \sum_{i=1}^{n}(x_i^2 + y_i^2 - 2x_iy_i) = A + B + C$$

Decryption is computed such that

$$\psi(\xi_r(m)) = \frac{L(c^\lambda \,\mathrm{mod}(N^2))}{L(g^\lambda \,\mathrm{mod}(N^2))} = m \,\mathrm{mod}(N)$$

where $\lambda = \mathrm{lcm}(p - 1, q - 1)$ and $L(x) = \dfrac{x - 1}{N}$.

Barni et al. (2010)

Barni et al. proposed a homomorphic cryptosystem that facilitated the matching of fingerprint templates in the encrypted domain.

Method

At a high level, the proposed encryption method consists of three stages. In the first stage, the image is captured and processed into a template. For each transaction the user presents a fingerprint image to an acquisition device, and features are extracted from the query image to obtain a template whose structure reflects that proposed by Jain et al (2000).[45] In the second stage, the template is quantized. Both the first and second stages significantly influence the verification performance of the system. In the third stage, the quantized template is encrypted with a public-key on the server using a homomorphic cryptosystem. Matching occurs in the encrypted domain.

The proposed encryption protocol, which is executed in the third stage of the method, incorporates elements of the Paillier protocol and the ElGamal protocol using elliptic curves to preserve bandwidth. The distances between the quantized query vector and the vectors in the dataset are computed in the encrypted domain using these two cryptosystems.[46] If simply accepting or rejecting the user based, the servers computes

$$\llbracket R \rrbracket = r \cdot \left\llbracket \sum_{i=1}^{n} b^i \right\rrbracket = (\prod_{i=1}^{n} \llbracket b^i \rrbracket)^r$$

where r is a random integer. The user will be rejected if $\llbracket R \rrbracket = 0$.

Performance

The researchers tested the proposed method against 408 fingerprint images. The results yielded 6.5% EER. At the configuration necessary to achieve this level of accuracy, they were able to identify 80-bit templates in a dataset of 100 templates in 45.58 seconds at a quantization step of 4. Computations were conducted on machines with 2.4 GHz processors and 4GB RAM.

Huang et al. (2011)

Huang et al. proposed an encryption method that they claimed was computationally efficient. The proposed method uses homomorphic encryption, oblivious transfer, and garbled circuits.

Method[47]
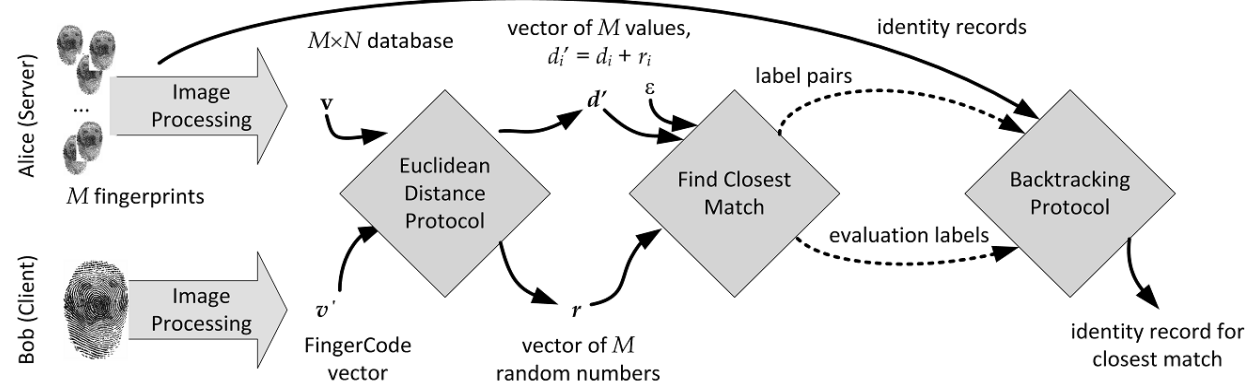
Figure 16: System overview (2011: 3)

[45] See A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, 2000, "Filterbank-based fingerprint matching," *IEEE Transactions on Image Processing*, vol. 9: 846–859.
[46] The protocol is discussed in Mauro Barni, 2010, "Privacy-Preserving Fingercode Authentication," in *12th ACM Multimedia and Security Workshop*.
[47] Source code for the software is freely available at http://www.mightbeevil.org/secure-biometrics/

At a high level the proposed protocol consists of three stages. First is to securely measure the Euclidian distance between the query and storage templates. Second is to securely match the encrypted templates. The third stage is to obliviously transfer the match results. To preprocess the images, the researchers used the filterbank approach proposed by Bazen et al. (2000).[48]

The Euclidian distance measurement protocol is based on an additively homomorphic encryption scheme. The server inputs a vector matrix $[v_{i,j}]_{M \times N}$ and the client inputs a single feature vector $[v'_q \ldots v'^1_N]$. The distance d_i between the stored vector v_i and the query v' is expressed verbosely as

$$d_i = \|v_i - v'\|^2 = \sum_{j=1}^{N}(v_{i,j} - v'_j)^2 = \underbrace{\sum_{j=1}^{N} v'^2_{i,j}}_{S_{i,1}} + \underbrace{\sum_{j=1}^{N}((-2v'_{i,j} \cdot v'_j))}_{S_{i,2}} + \underbrace{\sum_{j=1}^{N} v'^2_j}_{S_3}$$

resulting in a distance vector $d=\{d_1,d_2,\ldots,d_M\}$. The server transfers the data to the client using a garbled circuit protocol. It begins with knowledge of the distance measurements d and generates a set of nonce masks $r=[r_1,r_2,\ldots,r_M]$ and then sends the client

$$[\![a'_1\|\ldots\|a'_m]\!]_{pk} = [\![([a]_1 + r_1)\|([a]_2 + r_2)\|\ldots\|([a]_M + r_M)]\!]_{pk}$$

where pk is the client's public key. The sampling range of r_i should be large enough that d'_i and d_i are statistically indistinguishable. A backtracking protocol is used to transfer the match results. The protocol ensures that the server gains no knowledge of the data and the client gains nothing other than the data associated with the closest match.

Performance

The researchers tested the computational efficiency of their method. They claimed the method performed with 4.6 times the speed and 58% of the bandwidth of the method proposed by Barni et al. (2010). The tests were conducted on similar machines, with 2.0 GHz processors and 4GB RAM. Distance measurement accounts for a majority of the processing time, and circuit garbling accounts for a majority of the bandwidth. They did not test the verification performance of their protocol.

Further Reading

Huang, Yan et al. 2011. "Efficient Privacy-Preserving Biometric Identification." *18th Network and Distributed System Security Symposium*. http://www.mightbeevil.org/secure-biometrics/ndss-talk.pdf.

---

[48] See A. Bazen, G. Verwaaijen, S. Gerez, L. Veelenturf, and B. van Der Zwaag, 2000, "A Correlation-Based Fingerprint Verification System," in *ProRISC2000 Workshop on Circuits, Systems and Signal Processing*.

4.5   Local Aggregation

Local aggregation is a means of extracting features from a biometric input by counting the number of features that appeared within the confines of many randomly generated regions superimposed the input. Figure 17 illustrates this concept, where each element in the set contains the number of features found in one of the randomly superimposed regions. Regions are generated according to a secret key that is unique to every user. This implies that each user has a unique but repeatable pattern of random regions. If someone were to present a stolen image without its corresponding key, features would be counted incorrectly and the imposter would be invalidated.

Figure 17: Local aggregation methods generate sets based on minutiae in each random region

Templates produced by this method can be cancelled by reenrolling the biometric with a different key, resulting in a new pattern of random regions. The method is considerably tolerant to intraclass variations because it checks only for the presence of features within wide regions. Intraclass variations due to minor rotation, translation, and warping are not likely to push the features outside the boundaries of the regions as long as the input is aligned. Cryptographic keys are computed from metrics like the number of minutiae points within each region, which are easier to reproduce in subsequent transactions than the exact coordinates and angles of the minutiae points. Overall this method possesses the advantage of computational simplicity. Furthermore, because this approach does not transform the biometric features, it avoids producing inadvertent errors due to arbitrarily or unreliably designed transform functions.

4.5.1   Articles

Sutcu et al. (2008)

Sutcu et al. applied the Slepian-Wolf error correction framework to encrypt fingerprint templates.[49] The proposed method counts the number of minutiae points from multiple, randomly placed regions of the fingerprint template to generate binary feature vectors appropriate for low-density parity check (LDPC) syndrome coding, a belief propagation algorithm.[50]

Method

At a high level, three steps constitute the enrollment and authentication stage. First, a feature map is extracted from an acquired fingerprint image. Second, a transform function maps the minutiae points to a binary feature vector. Finally, a syndrome encoding function maps the binary feature vector into a secure syndrome. The dataset stores the secure syndrome, the LDPC code, and a cryptographic hash of the binary feature vector.

---

[49] See D. Slepian and J.K. Wolf, 1973, "Noiseless Coding of Correlated Information Sources," in *IEEE Transactions on Information Theory*: 471-480.
[50] See Robert G. Gallager, 1963, "Low-Density Parity-Check Codes."

For each transaction the user presents a fingerprint image from which a feature vector M=(x$_i$,y$_i$,è$_i$) is extracted where x$_i$,y$_i$,è$_i$ respectively indicate the coordinates and angle of the minutiae points. The number of minutiae p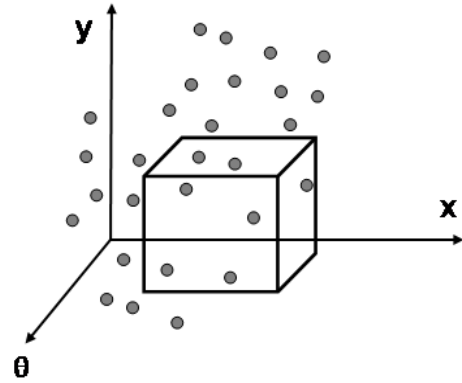oints is counted within multiple cuboidal regions randomly superimposed on the feature vector. Figure 16 illustrates the manner in which the regions are superimposed. If the number of minutiae points within a given region is less or greater than a predefined threshold, a bit value of 0 or 1 is respectively appended to the feature vector. In an enrollment transaction, a Slepian-Wolf encoder generates a syndrome from the feature vector and stores the syndrome in a dataset. In an authentication transaction, the LDPC decoder combines the secure template s and the query template b and applies belief propagation. The result is a an estimate $\hat{a}$ of the enrolled feature vector a. Access is granted to the user if the hash values of $\hat{a}$ and a match.

Figure 18: Example of a randomly placed cuboidal region containing seven minutiae points (2008: 4).

Performance

The researchers tested the proposed method against 1,035 prealigned minutiae maps from 69 fingerprints. They achieved as low as 11% FRR at 0.01% FAR, meeting at 2.7% EER. At this level of accuracy the protected template possessed 30 bits of security. Its accuracy is owed in large part to the prealignment of the fingerprint template.

Jin et al. (2009)

Jin et al. produced cancelable fingerprint templates by counting the number of minutiae points within randomly generated regions superimposed on the acquired image. They claimed the method was resistant to minor intraclass variations due to translation and rotation. The proposed method required no prealignment of the images because the minutiae are projected onto a two dimensional space according to reference minutiae.

Method

Minutiae points M$_i$=(x$_i$,y$_i$,è$_i$) are extracted where x$_i$,y$_i$,è$_i$ respectively indicate the coordinates and angle of the minutiae points. One minutiae point M$_r$ is selected as a reference point by which all other minutiae points will be translated such that

$$\begin{bmatrix} x_i^t \\ y_i^t \\ \theta_i^t \end{bmatrix} = \begin{bmatrix} x_i^t & x_i^t & 0 \\ y_i^t & y_i^t & 0 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} x_i - x_r \\ -(y_i - y_r) \\ \theta_i - \theta_r \end{bmatrix} + \begin{bmatrix} W \\ H \\ 0 \end{bmatrix}$$

where W and H are the width and height of the image. This translation centers the minutiae points around the reference point, which ultimately allows the proposed scheme to tolerate intraclass variations. The number of minutiae points within the confines of each random region is stored on a vector. The researchers used triangular regions to preserve computational simplicity. They surmised that other shapes were unlikely to enhance entropy or matching accuracy; rather they found that error rates could be reduced simply by increasing the number of regions.

The server assigns a unique, secret key to every user during enrollment. The key is a set of random numbers that determines the shape and location of several triangular regions to be superimposed on the image. In the event that a template is compromised, the key can be reissued to cancel the compromised template and enroll a new one. Within each triangular region, the number of minutiae points falling within an angular range is recorded to a vector. Figure 17 illustrates this concept, where the number of minutiae points is counted per angular range within a superimposed region. The feature vectors for multiple random regions are concatenated into a bit string.
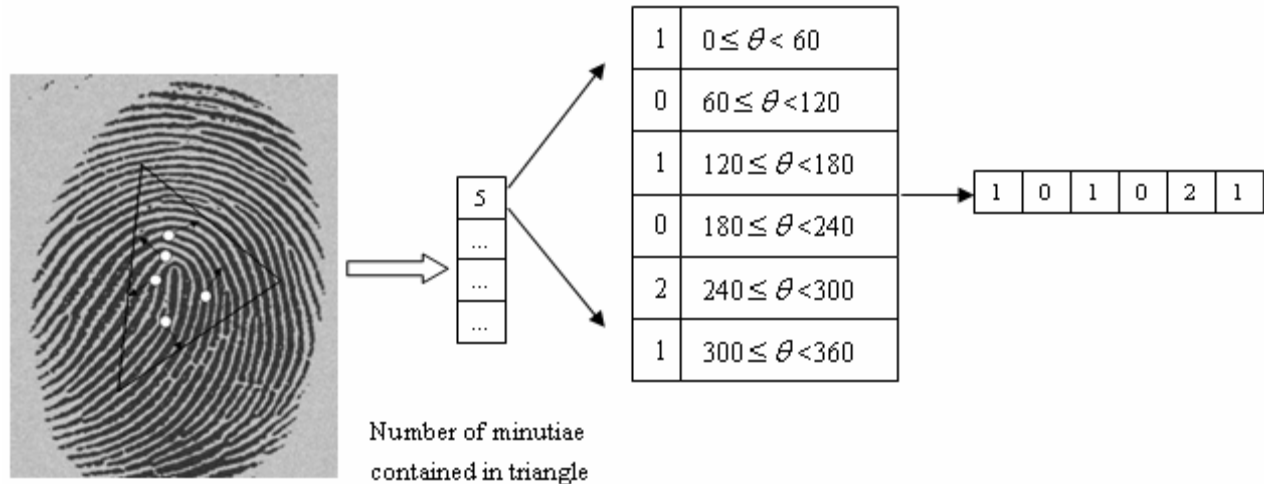
Figure 19: Bit string as function of minutiae points per angular range per random region (2009: 526)

Performance

The researchers tested their method against 800 fingerprint images, using VeriFinger Standard SDK to extract the minutiae coordinates. They achieved 2.81% EER where 10 random triangles were used and 0.20% EER where 20 random triangles were used. In the proposed method, the principal tradeoff for security was computational time, not matching accuracy. The researchers briefly mentioned that in a stolen-token scenario, EER can increase to more than 10%. The security of this method as it pertains to stolen tokens should be evaluated. This method is computationally simple compared to others reviewed in this report.

Nagar et al. (2010)

Nagar et al. proposed a method to secure fingerprint templates following the methodology of Sutcu et al. (2008). They extended the method to extract both the minutiae points and the fingerprint ridges.

Method

For each transaction, the user presents a fingerprint image from which a feature vector is extracted as shown in Figure 20. If the algorithm is developed to extract minutiae points, the feature vector will consists of x_i, y_i, θ_i which respectively indicate the coordinates and angle of the minutiae points. If developed to extract fingerprint ridges, the feature vector will consist of x_i, y_i which represent the coordinates of the ridges. Geometric regions are randomly superimposed on the feature vector and the number of minutiae points or fingerprint ridges is counted in each region. Figure 20 illustrates this concept. For each region, three measurements are recorded when selecting minutiae points: (1) the sum of the closest distance of each minutiae point from the regional boundaries; (2) the average coordinate of all the minutiae present in the region; and (3) the standard deviation of the minutiae coordinates present in the region. If the number of features is less or greater than predefined median thresholds for these values, then a respective bit value of 0 or 1 is appended to the binary feature vector. The binary feature vector is curated such that only the most reliable bits are extracted. The bits are altered by a low density parity check, and the final output, a secure syndrome, is stored in the dataset.

Performance

Figure 20: Example of local aggregation from randomly superimposed regions.[51]

The researchers tested their method against 800 fingerprint images from the FVC2002 Dataset-2, generating 500 random cuboidal regions per finger. They achieved as low 2% EER under normal circumstances, when an imposter has now knowledge of the template. Results fell to 3%EER when an imposter has knowledge of discriminable feature bits, and were worst at 10.2% EER when the imposter had knowledge of the aggregate wa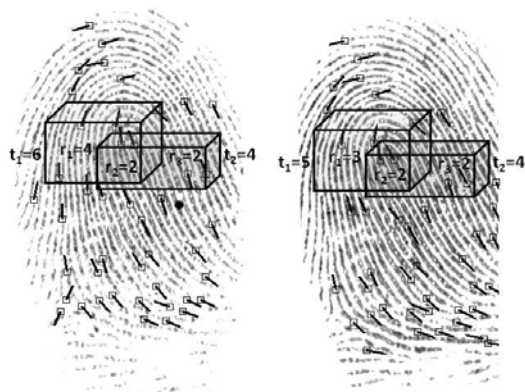ll distance. These results suggest that the method is robust against attacks whereby an attacker has knowledge of some, but not all, of the template information. These results signify a slight increase in accuracy compared to Sutcu et al. (2008), although this could be due in part to the prealignment of the fingerprint images.

4.6   Multifactor Key Generation

Multifactor key generation combines a biometric with one or more other inputs, such as a password or token, to produce cryptographic keys. This approach is essentially a form of salting, whereby the user supplies secret auxiliary information that that influences the transformation of the biometric image or template. Combining biometrics with other authentication factors has proven to be a reliable means of generating secure templates or cryptographic keys.

From a security perspective, this method is advantageous because it combines something that the user is with something that the user has or knows. The principal tradeoff for security in multifactor key generation protocols is usability, not necessarily verification performance. Access control systems that use multifactor key generation could easily become a hassle to users who forgot their password or token. Furthermore, the need to present multiple inputs during authentication is impractical for applications like security checkpoints.

4.6.1   Vulnerabilities

Stolen Token

Theoretically the security of the encrypted template is no greater than that of least secure authentication factor, assuming that any authentication factor can stolen and used by an imposter. Kong et al. (2010) criticized the method by Teoh et al. (2004), known for having achieved 0% EER, in which biometric inputs are irreversibly transformed by tokenized random numbers. The critics argued that the method lost any practical security when the token was stolen, thereby rendering the token redundant. Teoh et al. (2004) introduced multispace random projections as a means to harden the original method against stolen token attacks.

4.6.2   Performance

Empirical results on multifactor key generation have produced mostly good results. It has been tested on fingerprint, iris, face, voice, keystroke and multimodal biometrics. Teoh et al. (2004) reported perfect match rates from their experiment on fingerprint hashing, though they produced inconsistent results in subsequent studies. Some researchers argued that the high performance of schemes combining biometrics with a stored or known input were owed entirely to that second input; and therefore it was redundant to include biometrics in the key generation process.

---

[51] From Abhishek Nagar, Shantanu Rane and Anthony Vetro, 2010, "Privacy and Security of Features Extracted from Minutiae Aggregates," Mitsubishi Electric Research Laboratories.

4.6.3 Articles

Monrose et al. (2001a)

Monrose et al. proposed a multifactor key generation protocol that analyzed the keystroke dynamics of users as they typed passwords. If the keystroke pattern did not match the pattern recorded during enrollment, the system would not authenticate the user even if the password was correct. The proposed method adapts to changes in the typing pattern of a user over time.

Method

Each user account stores two data structures: (1) an instruction table containing $\langle i, á_{ai}, â_{ai} \rangle$ for each feature $\phi i\ (a,l)$ that controls how the algorithm will harden the password using the biometric features; and (2) a symmetrically encrypted history file that contains measurements on all features recorded over some number of successful logins. For each feature $\phi i\ (a,l)$ the login program uses "pwd'" to decrypt $á_{ai}$ or $â_{ai}$ such that

$$(x_i, y_i) = \begin{cases} (2i, \alpha_{ai} \cdot G_{pwd'}(2i)^{-1} \bmod q) & \text{if } \phi(a, l) < t_i \\ (2i + 1, \beta_{ai} \cdot G_{pwd'}(2i + 1)^{-1} \bmod q) & \text{if } \phi(a, l) \le t_i \end{cases}$$

where q is a large prime number,[52] G is a pseudorandom function family.[53] This creates m points $\{(x_i, y_i)\} \le i \le m$. The login program, then decrypts the history with an algorithm hwpd' such that

$$\text{hwpd}' = \sum_{i=1}^{m} y_i \cdot \lambda_i \bmod q$$

where $ë_i$ is the Lagrange coefficient for interpolation, expressed as

$$\lambda_i = \prod_{1 \le j, j \ne i} \frac{x_j}{x_j - x_i}$$

If the hardened password decrypts the history file, the history file is updated to include the keystroke dynamics of the current login attempt and computes the standard deviation of all keystroke dynamics contained in the file. The researchers measured the duration of keystrokes and the latency between keystrokes in their implementation. They designed two variations of the proposed system: one used exponentiation[54] and the other used vector spaces.[55] These variations addressed several security vulnerabilities observed in the foundational approach described above.

Performance

The researchers tested their method against 188 authentication attempts on a program that associated users' keystroke dynamics with their passwords. The results yielded 48.4% FRR where ~12 distinguishing features were recorded and 22.9% FRR where ~7 distinguishing features were recorded. This approach has an advantage of

---

[52] 160 bits is sufficient, p. 3.
[53] See R. L. Rivest, "Cryptography," *Handbook of Theoretical Computer Science*, pp. 717-755.
[54] See pp. 5-6 for details on the variation using exponentiation.
[55] See pp. 6-7 for details on the variation using vector spaces.

usability compared to other multifactor schemes like BioHash because the user does not have to supply two forms of information; for the biometric data is acquired automatically upon typing the password. However, due to its reportedly high error rates, it is likely that a legitimate user must input their password multiple times before the system authenticates them. The entropy of the hardened password depends on the entropy of the input password and the number of distinguishing characteristics parameterized in the keystroke analysis algorithm.

Monrose et al. (2001b)

Monrose et al. built upon their multifactor key generation scheme whereby a password is hardened by biometric data acquired during enrollment. They had applied their scheme to the keystroke biometrics, which meant that the input password consisted of an unambiguous sequence of characters. In this paper, the researchers attempted to apply their method to vocal biometrics. This presented a new challenge. Unlike passwords, vocal utterances vary for each transaction. Therefore the encryption of vocal characteristics was more complicated than merely running the input through a hash function. The authors were not satisfied by merely hashing a password extracted from by automatic speech recognition. Instead the proposed method attempted to recognize how a user uttered the password, storing the vocal features in a protected set. This allowed the system to verify identities based on vocal characteristics.

Method

During enrollment, the user utters a phrase and the vocal sample is segmented into 30-ms frames. Each frame corresponds to one component sound of the utterance. Silent frames are discarded. The segments are then mapped onto a set of features. An m-bit feature descriptor is derived from the segmented features. The researchers described three algorithms for extracting features but only reported on one that depended on the position relative to a plan through the centroid. The algorithm allowed them to produce 46-bit keys from two-second utterances. The algorithm can be expressed as

$$b(i) = \begin{cases} 0 & \text{if} \quad \alpha \cdot (\mu(R_i - c(R_i)) < 0 \\ 1 & \text{if} \quad \alpha \cdot (\mu(R_i - c(R_i)) \geq 0 \end{cases}$$

where á is a fixed vector, ì(R$_i$) is a vector of the average values of the segment frames, c(R$_j$) is the centroid, and b(i) represents the position of ì(R$_i$) relative to the plane á·x=0 translated to a coordinated space whose origin is c(R$_i$). The resulting feature descriptor is a bit string.

Performance

The researchers tested the proposed method against 250 utterances. The proposed method achieved < 5% FRR where k=1.875 and v=0.25, and < 30% FRR where k=1.250 and k=0.95. In general, the number false rejects increased as k decreased and as v increased. It may be noted that telephones were used to acquire the biometric samples to the detriment of matching performance. Like their previous method, this multifactor key generation scheme has the advantage of usability. Both the password and the biometric are acquired in the same action.

Teoh et al. (2004)

Teoh et al. hypothesized that a multifactor key generation method that integrated biometrics with known inputs would safeguard the privacy of biometric data without significantly decreasing verification performance. They argued in favor of combining biometric data with a tokenized random number rather than a password which is more susceptible to theft, to generate or match an encrypted biometric template. Guided by this hypothesis the researchers developed an encryption method called "BioHash," wherein fingerprint minutiae and a tokenized random number both influence the generation of a cryptographic key. The proposed method remains one of the top performers in terms of error rates relative to other empirical test results reviewed in this report.

Method

The proposed method involves two general steps: first to segment the biometric features, then to hash the features

using the tokenized random number as an influencing parameter. The researchers applied an integrated wavelet transform and a Fourier-Mellin transform to segment the fingerprint minutiae. Then they aligned the images to achieve a common size, angle, and position.[56] The resulting feature data was altered by a quantization process, which consist of four steps:

1. Derive a pseudorandom number $\{r_i \in R^M \mid i=1,\ldots,m\}$ from the token.

2. Apply the Gram-Schmidt process to transform the pseudorandom number into an orthonomal set of matrices $\{r_i \in R^M \mid i=1,\ldots,m\}$.

3. Compute $\{\langle \tilde{A}|r_i \in R^M \rangle \mid i = 1,\ldots,m\}$.

4. Compute m-bit BioHash $b_i \in 2^m$ such that

$$b_i = \begin{cases} 0 \text{ if } \langle \Gamma | r_i \rangle \leq \tau \\ 1 \text{ if } \langle \Gamma | r_i \rangle > \tau \end{cases}$$

where τ is a predefined threshold. This quantization process distinguishes the BioHash method from other template protection methods. Upon executing the wavelet transforms and discretization algorithm, the end product is a template that cannot feasibly be reverse engineered without presenting both the biometric image and tokenized random number.

Performance

The researchers tested the proposed method against 600 fingerprint images, conducting 29,700 imposter attempts and 1,500 genuine attempts. They claimed to have achieved 0% EER where the bit length of the template was equal to or greater than 40. The results implied that the approach is reliably error-tolerant and perhaps the most robust of all those reviewed in this report. But they were contested by several academics. Cheung et al. (2005) could not reproduce high quality match rates using the proposed transform method, feature extraction method, and similarity measure. Kong et al. (2006) argued that 0% EER was owed entirely to the tokenized random number; therefore to integrate biometrics with a token would be redundant as the token alone sufficed as the perfect password. Having tested the method in a stolen-token scenario, the critics observed it to distinguish genuine and imposter users very poorly.

In defence of their methodology, Teoh et al. (2007) published the match rates of their method in stolen-token and stolen-biometrics scenarios using two different feature extraction methods. In the stolen-biometrics scenario, they achieved 2.11% EER and 0% EER respectively; whereas in the stolen-token scenario they achieved 26.79% EER and 21.53% EER. BioHash and its variants thus remain vulnerable to imposters who wield stolen tokens. The researchers proposed a multistage approach to their method that enhanced the matching performance in the event of a stolen token.[57]

Hao et al. (2006)

Hao et al. proposed a method for encrypting iris images in such a way that produced error-free keys despite the

---

[56] See pp. 2248-9 for a detailed example of the transforms used.
[57] See pp. 2040-2.

typical 10-20% error bits found in iris codes. They hypothesized that correcting errors in biometric data using Reed-Solomon and Hadamard codes prior to matching would improve performance without sacrificing security.

Method

The proposed method, as shown in Figure 21, encompasses two aspects: an error-correction code that combines Reed-Solomon and Hadamard codes, and multifactor key generation using an auxiliary secret, e.g. a password. The Reed-Solomon code corrects errors in the input image at the block level, and then the Hadamard code corrects errors at the binary level. An XOR operation between the binary string θ_{ps} a reference iris code θ_{ref} produces an encrypted template θ_{lock} to be saved on a smartcard or other token, defined as

$$\theta_{lock} = \theta_{ps} \oplus \theta_{ref}$$

To decrypt the key, an XOR operation between an input image and the encrypted template is executed such that

$$\theta'_{ps} = \theta_{lock} \oplus \theta_{sam}$$
$$= \theta_{ps} \oplus e$$

where e is the error vector between two iris codes. Error correction recovers the trial value of the biometric key $\hat{k}$ and a match exists where e is within the correction capability $\hat{k} = k$, which is verified by comparing the hash values.
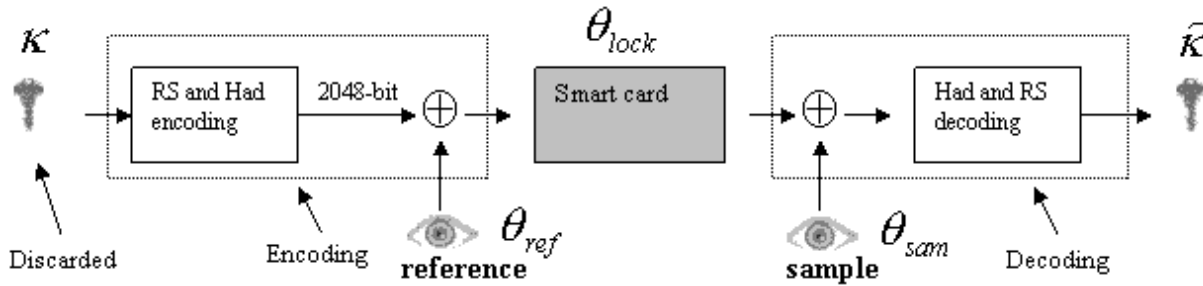
Figure 21: Schematic overview of the proposed system (2006: 8).

Performance

The researchers tested the proposed method against 700 iris images. Where block length was equal to six, they achieved 0% FAR and 0.47% FRR from 241,300 imposter comparisons and 3,150 genuine comparisons. These among the best results of the studies reviewed in this report. They noted that the Hadamard code caused a tradeoff between error tolerance and key length. Thus while they achieved an even lower false rejection rate where the block length equaled seven, the loss in entropy made the key less than optimal.

Ballard et al. (2008)

Ballard et al. observed a tendency for some biometric modalities to produce highly entropic keys.[58] The objective of their research was to create highly entropic keys regardless of the modality. They proposed a multifactor key generation method that augmented the entropy of the key.

---

[58] See, e.g. Monrose et al. (2001a) and

Monrose et al. (2001b).

Method[59]

Two algorithms constitute the method: enrollment and key generation. During enrollment, the user presents a biometric B and a password. Having extracted the features from the input, their statistical characteristics are calculated and an index of each feature is stored in a table. Error correction codes quantize the range of the feature into partitions of a length equal to the quantization width δ_i of the map from theset of biometric samples

$$\alpha_i = \begin{cases} \left\lfloor \mu_i - \frac{\delta_i}{2} \bmod \delta_i \right\rfloor & \text{if} \quad \mu_i \geq \frac{\delta_i}{2} \\ \left\lfloor \mu_i + \frac{\delta_i}{2} \right\rfloor & \text{if} \quad \mu_i < \frac{\delta_i}{2} \end{cases}$$

where ì is the median of each feature $\phi(\hat{a}_1), \ldots, \phi(\hat{a}_l)$. The key is derived from a random oracle applied to the

password, the feature indexes, and the lower boundaries of the partition that contains the output of each feature. The feature data and quantized outputs are encoded into secure template. The template T consists of the encrypted feature set C and token v such that

$$T = (C, v) = ((C_1 0, C_1 2, \ldots, C_1(n-1)), H_1 \text{"ver"} \; (\pi|(|K_1\sigma|)|\ldots||K_1(m-1)))$$

where K is a cryptographic key and ð is an optional password serving as an extra source of randomness. During authentication, the user submits a query biometric and password with which the key generation algorithm will attempt to decrypt the stored template. If the key matches the token in the stored template, the algorithm can recreate the list of feature indexes and quantization offsets. The system can only return a match if the key generation algorithm quantizes the output range of the features in the same way the enrollment algorithm does.

Performance

The research tested the proposed method against human forgers and the concatenative synthesis generative algorithm.[60] Respectively, they achieved as low as 17.7% EER against human forgers and 27% EER against the CS algorithm. Such results suggest that the method is not suitable for practical applications.

Kanade et al. (2010)

Kanade et al. proposed a method for encrypting multimodal biometric templates whose keys possessed greater entropy than those produced in previous methods. As such their study is similar in its objectives and methodology to that of Merkle et al. (2010).

Method

The researchers used two layers of error correction in the enrollment phase. First they used Reed-Solomon codes, then Hadamard and BCH encoding for modality-specific error correction. They gave a higher weight to error correction for iris images because they have shown to produce fewer errors than fingerprint images. The output of the Reed-Solomon error correction is salted by a user specific secret. This salt serves as the cancelable property in the proposed method. The salted, error corrected output is then divided into two parts: one to be encoded by a Hadamard code, the other by a BCH code. Those outputs were concatenated and finally XORed with the concatenated uniform zero insertion values of the reference iris code and face code. During authentication, a query iris image undergoes uniform zero insertion and is concatenated with the face image input. This value is XORed

---

[59] Pseudocode for the enrollment and key generation algorithms are shown on p. 5.
[60] For details on concatenative synthesis, see L. Ballard, S. Kamara and M. K. Reiter, 2006, "The Practical Subtleties of Biometric Key Generation," in *Proceedings of the 17th Annual USENIX Security Symposium*: 29-41.

with the encrypted template, and the result is divided into two parts: one to one to be decoded by a Hadamard code, the other by a BCH code. The concatenated value must be "un-shuffled" by a password supplied by the user, and the resultant value will be decoded by Reed-Solomon codes. If successful, the result is a regenerated key. Figure 22 illustrates the overall workflow of the proposed method.
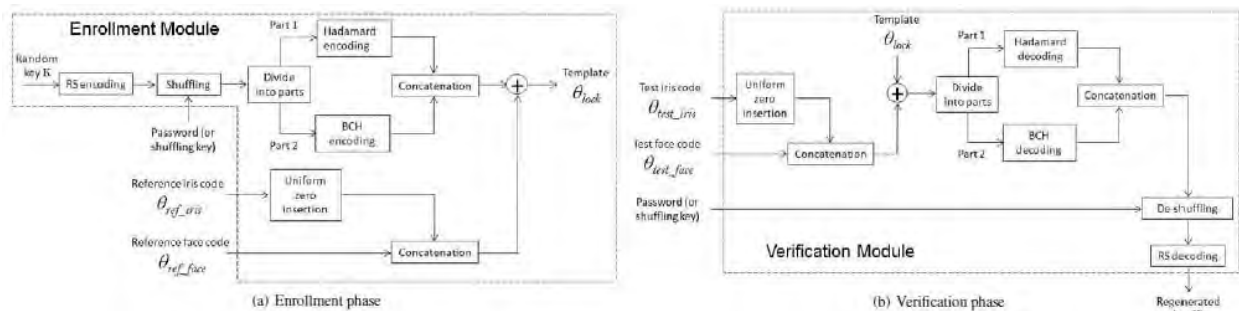
Figure 22: Schematic diagram of multifactor key generation enrollment and verification modules

Performance

Having tested the proposed method against 380,625 imposter comparisons and 1,750 genuine comparisons, the researchers were able to produce 210-bit keys at 0.91% FRR and 0% FAR and 168-bit keys at 0.11% FRR and 0% FAR. With a combined high level of entropy and low level of error puts, these results showed that the method effectively mitigated the tradeoff between template security and matching performance. These results suggested that a multimodal approach could effectively mitigate the tradeoff between template security and matching performance. Emerging now is a persuasive correlation between the quality of these results and those of the multifactor approaches.[61] It suggests that the encryption of any single biometric may not be enough to produce reliably secure and competent templates in many cases.

4.7 Noninvertible Transforms

Noninvertible transforms are a generic means of obfuscating biometric template data by way geometric transformation. Transforms are executed either at the single domain or the feature domain. The literature has favored feature domain transforms, which alter features such as the position of the minutiae coordinates. By contrast, single domain transforms alter the pixels of the raw image.

Figure 23 illustrates the manner in which minutiae points are repositioned by a feature domain geometric transform. The dots indicate the position and angle of fingerprint minutiae. Observe how they are repositioned after a Gaussian transform. Any template protection method could employ a noninvertible transform as one of several means of obfuscating the template data. Typically the parameters which influence the transform are used as the cancelable property in a protected template. For additional security, these parameters can be derived from a user-supplied input such as a password or a private key. The methods reviewed in this section use noninvertible transforms as the principal means of template protection.

---

[61] See Monrose et al. 2001; Teoh et al. 2004; Hao et al. 2006; Nandakumar et al. 2007; Ouda et al. 2010.
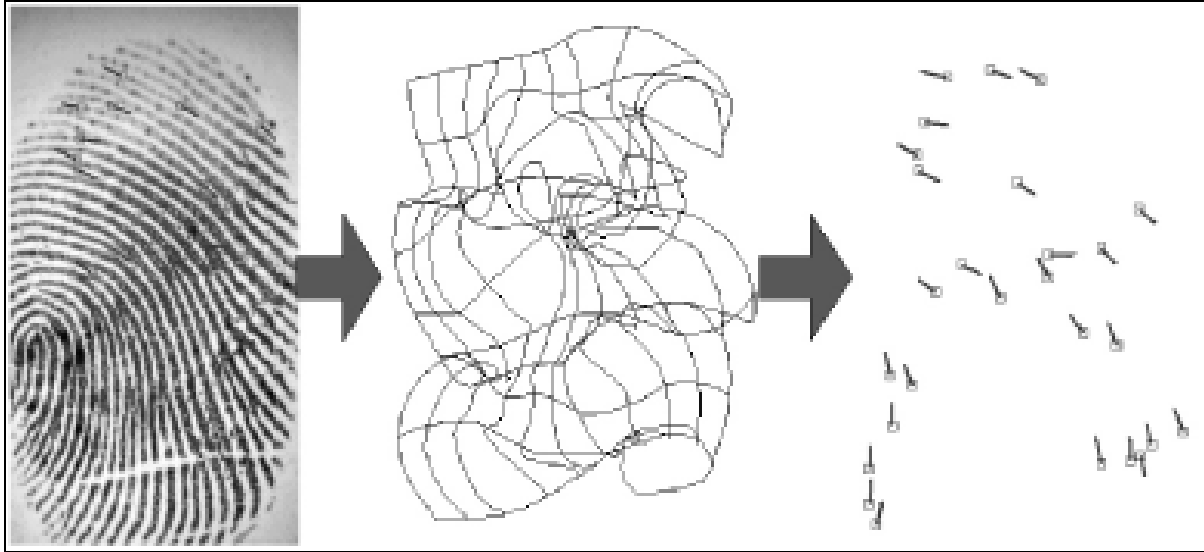
Figure 23: Example of a noninvertible transform (Nagar, Nandakumar and Jain 2006: 2).

4.7.1 Performance

It is difficult to compare the performance of methods that employ noninvertible transforms because the methods and transforms vary significantly. Hirata and Takahashi (2009) achieved extremely low error rates using correlation invariant random filtering. But no other transform-based method met the target of 1% FRR at 0% FAR, and many yielded double-digit error rates. Therefore this report will avoid making a blanket assessment of the performance of noninvertible transforms.

4.7.2 Articles

Soutar et al. (1999)

Soutar et al. reviewed an algorithm they developed at Mytec Technologies, Inc.,[62] in which fingerprint data fundamentally influenced the makeup of a private key. The algorithm, simply called Biometric Encryption, processed the entire image, not just the feature data, in the production and retrieval of a key. Their goal was to produce 128-bit keys, which could be used in common encryption standards like AES. They used a correlation filter function H(u) to measure the degree of similarity between input and reference images.[63] This, they claimed, helped to surmount the problem of intraclass variations but did not bolster the entropy of the key. They referred to the encrypted template as a Bioscrypt.

Method

At a high level, the user presents multiple fingerprint images to be transformed and linked with a cryptographic key during enrollment. An identification code is then stored in a lookup table. During authentication, the acquired image is again transformed. A key is retrieved from the lookup table, and the two identification codes are compared.

Two filters process the images: a filter function H(u) and a transitory filter. The filter function is defined as

$$H(u) = \frac{A_0^*(u)R(u)}{\alpha P(u) + \sqrt{1 - \alpha^2} \, D_0(u)}$$

---

[62] Mytec Technologies, Inc. has since been acquired by L-1 Identity Solutions.
[63] See J. W. Goodman, 1968, "Introduction to Fourier Optics"; A. VanderLugt, 1992, "Optical Signal Processing"; and E. G. Steward, 1995, "Fourier Optics: An Introduction."

where u is the spatial frequency domain, $A_o(u)$ and $R_o(u)$ is an array of random numbers.

During enrollment, the user presents T fingerprint images to train the system. [64] Fourier transforms are performed on each image to compute $A_o(u)$ and $D_o(u)$. An array of random numbers $R(u)$ is generated. The filter function $H(u)$ is responsible for ensuring low intraclass variance and high interclass variance. It produces an output pattern $c_o(x)$ that is linked with an N-bit key k_o. In this linking process, $c_o(x)$ is binarized and a lookup table is created and stored in the Bioscrypt to be used in key retrieval during authentication. Finally k_0 encrypts data from $H''stored''(u)$ [65] to be hashed and stored as an identification code id_o in the Bioscrypt. Thus the Bioscrypt consists of a lookup table, id_o, and $H_{stored}(u)$.

During authentication, the user presents T fingerprint images to be processed as in enrollment. Using $H_{stored}(u)$ from the Bioscrypt, an output pattern $c_1(x)$ is generated to be used in retrieving the N-bit cryptographic key.

Implications

This approach was tested on fingerprint images. The researchers noted that it could be applied to any modality as long as the data is represented as a two-dimensional array, like an image. Their method would eventually be implemented in the first commercial biometric template protection product called Bioscrypt. The method is more complex than many of the methods developed in successive research. Many critical details must be overlooked in summarizing it. Considering this, the method may be more expensive for systems to compute.

Ang et al. (2005)

Ang et al. designed a method for producing cancelable fingerprint templates. They applied a key-dependent geometric transform to the extracted features. Cancelling a template is a matter of changing the key used in the transform.

Method

During enrollment, the user presents a fingerprint from which a feature vector is extracted. Interested only in the design of the cancelable transform, the researchers preprocessed the image and extracted the features using VeriFinger SDK. For each minutiae point Mi a vector is built with the coordinates (x_i, y_i), angle φ_i, type t_i, and local feature vector $F_i = (d_{ij}, \theta_j, \varphi_{ij}, n_{ij}, t_j)$ for each neighbor minutiae point Mj where d_{ij} is the distance between Mi and a neighbor Mj, n_{ij} is the distance between their ridges, θ_{ij} is the angle between their ridges. Figure 24 illustrates the proposed feature vector when the number of neighboring minutiae points L=2.

Figure 24: Diagram of the local feature vector where L=2 (2005: 246

During verification, the user submits a query fingerprint from which a feature vector R is extracted, following the same model as in enrollment. The query vector F_i^R is compared against the stored vector F_i^T using a similarity function $s_l(i,j)$ where

---

[64] The researchers suggested 4 to 6 images to train the system sufficiently.
[65] They encrypted this data because it was unique to each user and present at both enrollment and authentication.

$$s_l(i,j) = \begin{cases} \dfrac{t_p - W.|F_i^T - F_j^R|}{t_p} & \text{if} \quad W.|F_i^T - F_j^R| < t_p \\ 0 & \text{if} \quad W.|F_i^T - F_j^R| \geq t_p \end{cases}$$

and where W is a weight vector for each element of F_i[66]. Ultimately the matching score M_s is expressed as

$$M_s = 100 \frac{\sum_{i,j} s_g(i,j)}{\max\{M, N\}}$$

The user is authenticated if M_s is higher than a given threshold T_P, the suggested value of which was $t_p = 6(5L+1)$

Performance

The researchers tested the proposed transform algorithm and matching algorithm against 800 images of 10 unique fingerprints, using the NIST Fingerprint Image Software to identify core points and extract the minutiae. They achieved 2% EER where the threshold $t_p = 0.53$ and 4% EER where $t_p = 0.52$.

Chen and Chandran (2007)

Chen and Chandran proposed a template protection that they claimed was more resistant to attacks than prior methods. As a benchmark they wanted to make the resultant keys compatible with the 128-bit Advanced Encryption Standard (AES). They also desired to make the template cancelable. The proposed method used Reed-Solomon error correction codes.

Method

---

[66] The methodology for calculating the weight vector was adopted from X. Jiang and W. Yau, "Fingerprint Minutiae Matching Based on the Local and Global Structures," in *Proceedings of the 15th International Conference on Pattern Recognition II* (2000): 6038–6041.
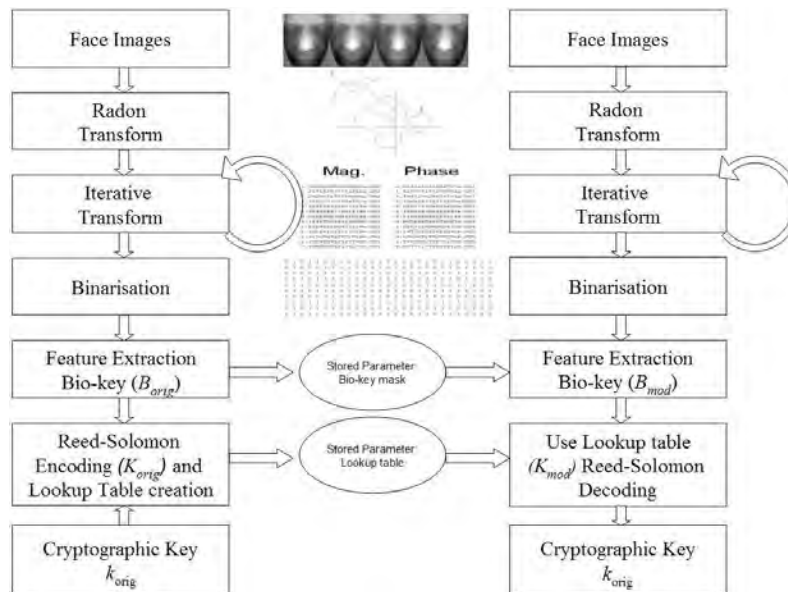
Figure 25: Schematic diagram of transform- and error-correction-based method (2007: 3).

As shown in Figure 25, upon enrollment, the biometric image undergoes a bispectral transform that is designed to eliminate bit errors. Specifically a Radon transform converts the image into an array of one-dimensional projections. Then an iterative, bispectral transform alters the projections in a noninvertible fashion.[67] The resultant magnitude and angle matrices are converted to binary form. The "desirable" bits, having high interclass entropy and low intraclass entropy, are selected from the binary matrices. Templates can be cancelled by changing the number of iterations or the criteria for bit selection. Finally a lookup table is constructed with the two columns of N-bit sequences—one for the original key, the other for the bio-key—which are encoded with a Reed-Solomon coding scheme.

Performance

The researchers tested their method against three dimensional face images, which were normalized. Without error correction codes, they achieved 66% FRR at 0.26% FAR where key length N = 64 and 95% FRR at 0.0006% FAR where N = 512. After implementing Reed-Solomon error correction codes, they achieved 25% FRR at 1.22% FAR where key length k = 112 and 63% FRR at 0.09% FAR where k = 208. Neither approach produced results that would suffice for most real-world applications. They predicted that to implement Hadamard error correction code before the Reed-Solomon code would improve the matching performance, and this was confirmed in the tests by Hao et al. (2006).

Boult et al. (2007)

Boult et al. generated cancelable tokens called Biotopes by applying a noninvertible transform to minutiae points. Having explained the basic protocol, they further described how to implement it in such a way that supported multifactor key generation. The term "Biotope" was eventually trademarked and used in biotoken products sold by Securics, Inc.

Method

---

[67] See V. Chandran and S. L. Elgar, 1993, "Pattern Recognition Using Invariants Defined from Higher Order Spectra: One Dimensional Inputs," in *IEEE Transactions on Signal Processing* (41): 205.
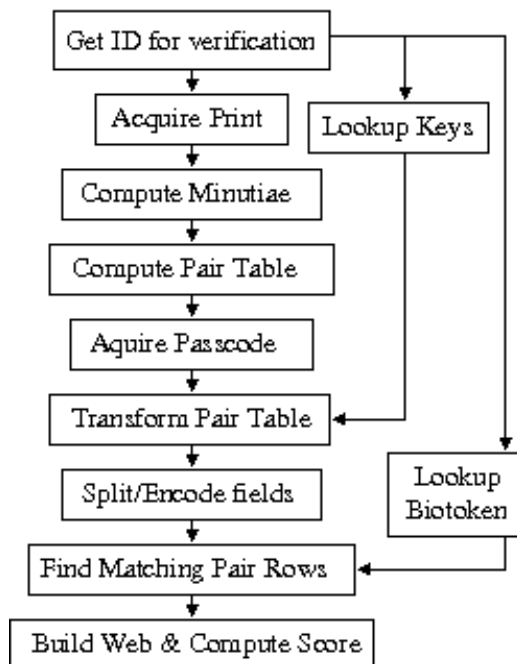
Figure 26: Schematic diagram of process for generating and matching biotokens (2007: 4).
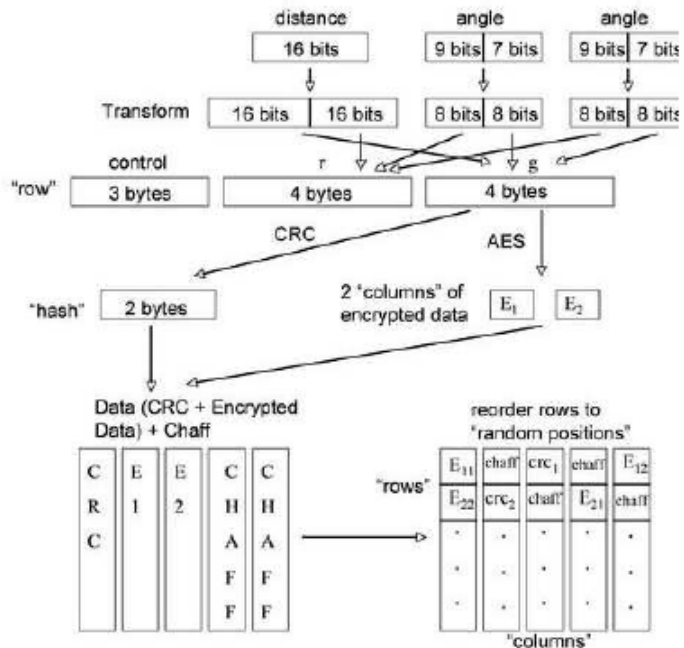
Figure 27: Schematic diagram of process for mapping data for use as biotokens (2007: 5).

Figure 26 and Figure 27 give a high level overview of the process for generating and matching tokens. Fingerprint features are first extracted from an input image. The researchers used a Bozorth matcher, which takes as input a feature vector $v=(x,y,\theta,q)$ where x,y,θ respectively indicate the coordinates and angle of the minutiae points and q is a measure of quality.[68]

Performance

The researchers tested both the proposed method and the NIST VBT method against 4,950 imposter fingerprints and 2,800 genuine fingerprints. The proposed method achieved 8.6%-1.2% EER and outperformed the NST VBT method by ~33%. Thus they claimed that the proposed biotoken method improved verification performance.

Scheirer and Boult (2008)

Scheirer and Boult proposed a form of cancelable biometric token or "biotoken" to be used in symmetric key release systems where both parties mutually validate the transaction. They designed the token to support one-time transactions and trust hierarchies. Furthermore they claimed their method allowed for better auditing, non-repudiation, and protection against replay, phishing and man-in-the-middle attacks. The public key is the only information ever reused in subsequent transactions. Using the proposed biotoken the researchers designed multiple protocols for secure transactions and digital signatures.

Method

Revocable Biotokens

For each transaction, the user presents a biometric image that is scaled, translated, and ultimately split into stable and unstable components, which are respectively called the quotient q and the remainder r. The quotient q is encrypted or hashed while the remainder r is left in the clear. Because the quotient q is stable, it can be used for exact matching. The measure of dissimilarity between two biometric signals d(p,q) is computed such that

---

[68] For details on the Bozorth matcher, see C.I. Watson et al., 2004, "User's Guide to NIST Fingerprint Image Software 2."

$$d(p, q) = \begin{cases} c & \text{if} \quad w(p)! = \text{abs}(r(p) - r(q)) \geq b \\ (\dfrac{r(p)}{s(p)} - \dfrac{r(q)}{s(q)})^2 & \text{if} \quad w(p)! = \text{abs}(r(p) - r(q)) < b \end{cases}$$

where c is a constant penalty to outliers.

Nested Biotokens

The researchers described a method for re-encoding biotokens, which builds hierarchies of trust and allows data to be released without revealing other secrets. In the same way that certificate authorities issue digital certificates in a hierarchy of trust, biotokens can be encoded multiple times to produce keys unique to specific applications. For each encoding, the transformed biotoken w_j is re-encoded with a unique transform function T. The process can be expressed as

$$
\begin{aligned}
&1\text{st encoding: } w_{j,1}(v', P) \\
&2\text{nd encoding: } w_{j,2}(w_{j,1}, T_2) \\
&3\text{rd encoding: } w_{j,3}(w_{j,2}, T_3) \\
&\ldots \\
&n\text{th encoding: } w_{j,n}(w_{j,n-1}, T_n)
\end{aligned}
$$

where P is a public key used to encode the biotoken in the first iteration.

Bipartite Biotokens

Bipartite biotokens assume properties of fuzzy cryptosystems. An embedded polynomial obfuscates secret data with chaff data. The biotoken is transformed in such a way that allows data to be secured in it and released upon successful verification. This method is covered in depth by Scheirer and Boult (2009).

Digital Signatures

The sensor sends a public key to a remote signature server, which returns a transaction ID. The sensor then sends the bipartite biotoken signature to the server, which will generate its own local biotoken and match the two biotokens. It sends the biotoken signature to the sensor, which validates the received signature and appends an audit log with server information. This process attempts to mitigate the man-in-the-middle attacks.

Maiorana et al. (2008)

Maiorana et al. encrypted handwritten signature templates, proposing the use of hidden Markov models to compare the templates in the encrypted domain.

Method

As the user writes a signature on the acquisition device, the features are extracted in the form of time sequences, whose parameters include: horizontal and vertical position trajectory (x_n, y_n), pressure signal p_n, path-tangent angle θ_n, path velocity magnitude v_n, log curvature radius $\tilde{n}_n$, and total acceleration magnitude a_n where n is a discrete time index. Altogether the time sequence vectors are expressed as

$$u_n = [x_n, y_n, p_n, \theta_n, v_n, \rho_n, a_n]^T, n = 1, 2, \ldots, N$$

Each time sequence vector u_n is stored in a template matrix $U = [u_1 \ldots u_N]$. A noninvertible transform function $f_i[n]$ is applied to elements in the matrix through the linear convolution of the functions $r_{(i)j, N1}[n]$ such that

$$f_i[n] = r_{(i)j,N_1}[n] * \ldots * r_{(i)W,N_W}[n]$$

producing a secure template T[n] of the transformed elements in u[n], such that

$$T=[f(u_1),\ldots,f(u_n)]$$

During authentication, the user writes a signature from which time sequence vectors are extracted. The representation of the query signature is compared against one or more secure signatures stored in the dataset using the Viterbi algorithm to calculate similarity score,[69] such that

$$\text{Score} = \left(\frac{1}{k}\right)\log P\!\left(\frac{T}{\lambda}\right)$$

where ë is the HMM model, defined by the number of hidden states H and the number of Gaussian densities M that describe the probability p(t) of the emission of symbol t from the state h,h=1,…,H.

Performance

The researchers tested the proposed method against 16,500 handwritten signatures. Results showed that this approach is not reliable. The method achieved its lowest equal error rate at 10.29% where the number of hidden states H=8, the number of Gaussian densities M=2, and W=2. The method may perform too poorly for most practical purposes until improvements are made; although it should be noted that the increase in EER was only slight compared to those of unprotected approaches.

Shi et al. (2008)

Shi et al. designed a framework that integrated feature extraction and noninvertible transforms in such a way that mitigated the tradeoff between security and performance. In their study they propose a feature extraction method called "MinuCode," which they claimed was more reliable than past methods. MinuCode avoids reference core point determination and deals with the noise of fingerprint biometrics.

Method

Shi et al. first extracted the minutiae coordinates and plotted them onto a polar coordinate system, forming a MinuCode template through a process shown in Figure 28. They used tessellation quantification to alter the coordinates in such a way that centered on a region of interest. Then they applied a noninvertible transform to the MinuCode T=(b,a,o). They described three possible transforms. The first transform involves three steps, where

$$k=(b\times p\times P\times P)+(a\times P\times o)$$

where P is a constant larger than a, b, or o. Then it encrypts a random string RS with a block cipher E_k () using k as the key. Finally publishes a new tuple $T^1=(RS,E_k(RS))$. The second transform involves two steps. First it generates three random positive integers r_1, r_2, r_3 and then it publishes a new tuple $T^n=(Z_1,Z_2,Z_3)$ with an application-specific parameter ë: $Z^1=b+r_1(a*P+o+ë)$, $Z2=a+r_1(a*P+b+ë)$, $Z^3=o+r_1(a*P+a+ë)$ where P is a constant larger than a, b, or o. The third transform discards r_1, r_2, r_3, and b, a, o. Before performing a match, the input images are automatically aligned using the minutiae-centered quotient calculation and tessellation quantification. Threshold mechanisms *tm* and *tp* are used to correct errors in minutiae locations: two regions are equal if there are at least *tm* equal neighbor minutiae, and finally two fingerprints are matched if there are at least *tp* equal regions.

---

[69] The researchers cite L.R. Rabiner, 1989, "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition," in *Proceedings of the IEEE* 7(2):257-286.
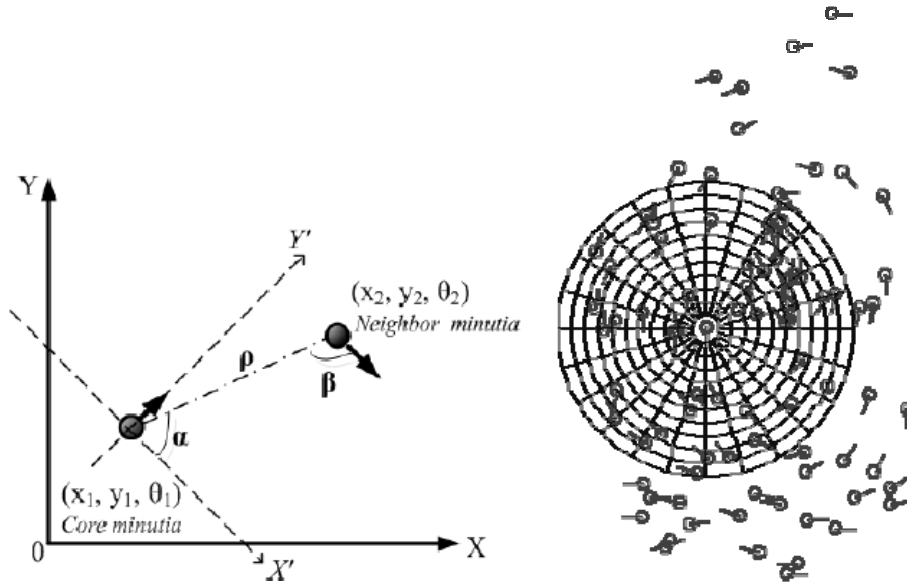
Figure 28: Illustration of MinuCode (2008: 2).

Performance

The researchers tested the proposed method against 800 fingerprint images. After 9,900 imposter comparisons and 100 genuine comparisons, their results yielded 1.35% EER. They were able to produce a 360-bit key, which is among the more secure keys of those reviewed in this report.

Hirata and Takahashi (2009)

Hirata and Takahashi, researchers at the Hitachi, Ltd. Systems Development Laboratory, produced cancelable templates with the goal of minimizing the tradeoff between security and performance. The researchers cited a prior study which found that a minimum average correlation energy filter could produce cancelable templates.[70] They used number theoretic transforms, which are similar to Fourier transforms and allow the system to match templates in the encrypted domain.[71]

Method

Assume the following preliminaries: $f(x,y)$ is the registered image; $g(x,y)$ is the input image; $F(u,v)$ is the number theoretic transform of the padded registered image; $G(u,v)$ is the number theoretic transform of the input image; $R(u,v)$ is a random filter; $R^{(-1)}(u,v)$ is the inverse of the random filter. The number theoretic transform ϕ has a cyclic convolution property of $\phi(a*b)=\phi(a)\phi(b)$ where $a=\{a1\}$, $b=\{b1\}$ and $*$ is convolution. This property facilitates correlation-based matching in the encrypted domain. The correlation between $f(x,y)$ and $g(x,y)$ is $w_{f,g}(p,q)$ expressed as

$$w_{f,g}(p,q) = \sum_{(x,y)\in S(p,q)} f(x-p, y-q)g(x,y)$$

where $S(p,q)$ is the region that the registered image overlaps the input image at the displacement (p,q). The system computes peak-to-mean from the correlation to authenticate the user. Peak and mean represent the maximum and mean values of $w_{f,g}(p,q)$ respectively, and the peak-to-mean ratio is simply peak – mean.

---

[70] See Savvides et al., 2004, "Cancelable Biometric Filters for Face Recognition," in *17th International Conference on Pattern Recognition (ICPR 2004)*, 3: 922-925.
[71] For details on the number theoretic transform, see R.C. Agarwal and C.S. Burrus, 1975, "Number Theoretic Transforms to Implement Fast Digital Convolution," in *Proceedings of the IEEE* 63(4): 550-560.

During enrollment, the user presents a fingerprint image. The client machine pads the acquired image and applies a number theoretic transform ø to the padded image. It multiplies the transformed image with a random filter, and the final product is sent to the dataset. The secure template can be expressed as $T(u,v)=R(u,v)F(u,v)$ where $R(u,v)$ is a uniformly random filter and $F(u,v)$ is the number theoretic transform of the padded input image. During authentication, the user presents a query fingerprint image. The steps are repeated and the server matches the input images against one or more registered templates in the encrypted domain.

Performance

The researchers tested the proposed method against infrared finger-vein images. Having conducted 102 genuine comparisons and 10,302 imposter comparisons, they achieved a complete separation between the normalized frequency distribution of the genuine and imposter classes, which implies 100% accuracy. They found small traces (0.016%) of information from the original images, though they claimed this was too small to allow one to reverse engineer an encrypted image.

<u>Takahashi and Hirata (2009)</u>

Takahashi and Hirata attempted to resolve the tradeoff between template security and verification accuracy. The proposed method adopts the correlation invariant random filtering approach proposed by Hirata and Takahashi (2009) into a chip matching algorithm proposed by Mimura et al.[72] This study culminated in U.S. Patent Application Publication 2008/0037833 A1.

Method

The researchers use a chip matching algorithm that builds upon their correlation invariant random filter (CIRF), which incorporates number theoretic transforms to achieve perfect secrecy.[73] The algorithm operates as follows:

(1) an input fingerprint image is processed to a binary image;
(2) the core is detected using the focal point method;
(3) minutiae coordinates are recorded in a set; and
(4) similarity between the chip image and the local area is measured by the Hamming distance.

Alignment of the input data is not required. As shownin Figure 29, during enrollment, the client machine preprocesses the fingerprint image from which the chip images will be clipped and filtered into a cancelable template to be stored on the server dataset. During authentication, the client machine presents an input image from which chips are clipped and filtered. The server cross-correlates each input chip and accept the user if the similarity score falls within a given threshold.

---
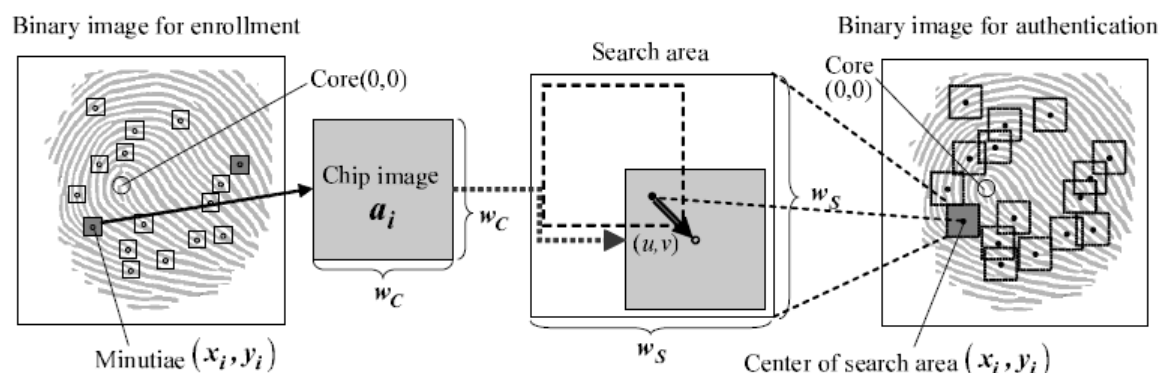
[72] See Masahiro Mimura, Shuichi Ishida, and Yoichi Seto, 2001, "Development of Personal Authentication Techniques Using Fingerprint Matching Embedded in Smart Cards," in *IEICE Transactions on Information and Systems*, E84-D(7): 812-818.
[73] See p. 2 for an overview of CIRF.

Figure 29: Illustration of the chip matching algorithm (2009: 3).

Performance

The researchers tested the proposed method with different parameter values against 181 fingerprint images. Results yielded 5.0% FRR at 0.2% FAR. These results were inferior to the previous implementation by Hirata and Takahashi (2009), which was tested against finger veins and did not incorporate a chip matching algorithm.

Scheirer and Boult (2009)

Scheirer and Boult designed a protocol that combined the methodologies of revocable biotokens by Scheirer and Boult (2008) and the fuzzy vault scheme by Juels and Sudan (2002). Like the fuzzy vault, the proposed method utilized Reed-Solomon error correction codes. But it did not store the points at which the secret polynomial was evaluated. It is allegedly rotation and translation invariant. The researchers defined bipartite biotokens as revocable fingerprint tokens that have been split into stable and unstable components, of which the former is encrypted or hashed and the latter is left in the clear.[74]

Method

For each transaction, the user presents a fingerprint image and the client machine sends a request for transaction to the server. The method uses a Bozorth-like procedure to conduct matching, where the raw distance and angles d,a_1,a_2 are stored in pair rows and their stable components sd,sa_1,sa_2 are protected in a lookup table. To evaluate the polynomial, sd,sa_1,sa_2 are hashed into a value i that is stored in the gallery. The hash digest i is again hashed as h in subsequent transactions, which is used only to evaluate polynomials to produce encoded bipartite rows. When matching a query against one or more stored templates, the system created all the fields for each of its rows, including the hash value h. A probe row potentially matches a gallery row if it finds a matching w and if the residual values rd,ra_1,ra_2 are within threshold. The algorithm evaluated the polynomial w generating potentially correct rs,rs_1,rs_2 values.

Performance

The researchers tested the proposed method against 750 million imposter attempts on fingerprint images. They achieved 3% FRR at 0% FAR with 256-bit security and 2 bytes of error correction. A biotoken with 16 rows and an error correction level of 6 can withstand up to 2^{480} brute force attempts, which represents an impressive girth of security.

The design of bipartite biotokens prevents cross matching, surreptitious key inversion (SKI), and blended substitution attacks. An attacker cannot cross-correlate biotokens even with access to the Reed-Solomon polynomial encodings, because the evaluation points are not stored within the encoding. The researchers note that the protocol was susceptible to an attacker whereby the attacker substitutes the columns of the biotoken with their own data, but they argued that this was a detectible action as it represents a denial of service to the genuine user.

4.8   Parametric Key Generation

Parametric key generation methods classify biometric features according to predefined parameters and generate a key derived from the parameter outputs rather than from the template itself. This approach mitigates the problem of intraclass variations because the shape and position of the features do not influence the construction of the encrypted template. For example, rather than store the locations of minutiae points, a fingerprint is classified simply as having an arch, loop, or whorl. Many parameters must be defined to ensure uniqueness among templates. The performance of any parametric key generation algorithm depends on the reliability of its parameters. A parameter is considered to be reliable if it consistently returns the same value upon many presentations of the same biometric. Therefore the best performing algorithms are likely to contain many parameters with simple definitions, allowing for many possible combinations and accurately reproduced queries.

---

[74] See p. 3 for a more extensive discussion on the definition of bipartite biotokens.

4.8.1 Vulnerabilities

Low Entropy

The strength of a parametrically generated key is a function of the number of parameters defined and the number of possible outputs per parameter. The number of parameters that can be defined is limited by our knowledge of ways to reliably classify biometric features. To illustrate, Hao and Chan. (2002) were unable to produce keys greater than an average length of 40 bits despite having defined 43 parameters. In their concluding remarks the researchers recommended appending additional data to the key as a means of augmenting its entropy. Such data could include a password or timestamp. The bare, single-factor methodology for parametric key generation is likely to produce low entropy keys vulnerable to brute force attacks.

4.8.2 Performance

Parametric key generation has not performed well in empirical tests, although the methods reviewed in this report were only applied to handwritten signatures which tend to yield higher error rates than other modalities like fingerprint and iris. None of the proposed methods met the target of 1% FRR at 0.1% FRR, but Chen and Chandran (2007) came reasonably close at 1% EER. Parametric key generation is not a reliable template protection method for most practical applications. The method may be best suited for small scale applications where there is limited computing power.

4.8.3 Articles

Hao and Chan. (2002)

Shortly prior to the time of this publication, electronic signatures were accepted as a legally binding under E-Sign (2000).[75] Thus began the boom of e-commerce and, more importantly, the now common practice of digitally authenticating oneself on computer networks. Hao and Feng attempted to apply biometrics to public key infrastructure (PKI), the convention by which digital information was secured. The difficulty they observed in such an implementation was the fuzzy nature of biometrics data. Because biometric images vary slightly upon each acquisition, no person could reproduce their own private key using cryptographic algorithms that demand precise inputs. They proposed a cryptosystem called BioPKI that attempted to circumvent this problem and produce secure and reliable private keys from biometric data.

Method

BioPKI consisted of three stages: shape matching, feature encoding, and private key generation. Shaping matching is a means of ruling out poor quality features by comparing the acquired image against "good" sample images. In their study, Hao and Feng applied dynamic time warping to align the shapes of handwritten signatures prior to shape matching. The biometric features are then extracted from the acquired image and encoded into a template. Lastly, private keys are generated from the encoded template using the digital signature algorithm (DSA). During enrollment, the algorithm produces an encrypted template and discards the original image so that none of the original data is stored. During authentication, a user presents a biometric image which is again encrypted and compared against one or more encrypted templates in the dataset. The templates can be matched only if the same transforms were applied to them, and the original data never needs to be revealed in order to verify an identity.

Performance

Hao and Feng tested their method against 750 handwritten signatures. They achieved 28% FRR at 1.2% FAR, meeting at 8% EER. Such results, while undesirable for practical applications, represented a promising start to the development of biometric cryptosystems. They reminded the readers of the naturally higher error rate of signatures compared to other modalities, such as iris. Therefore it would be worthwhile to test the approach on more common and reliable modalities. They were able to produce 40-bit keys, which is a weaker level of entropy compared to those in later template protection methods. They recommended padding the encoded template using information

---

[75] The Electronic Signatures in Global and National Commerce Act, enacted by the U.S. Congress in June 2000.

from the template or user supplied information (e.g. a password) prior to hashing it with the encryption algorithm. Doing so would fortify the key against brute force attacks and further guarantee uniqueness among keys.

Implications

The researchers mentioned the importance of all-bit-correctness when producing hash digests of biometric templates. Their solution to this was to define a set of parameters with a limited number of discrete values determined by the features of the acquired image. For example, pen pressure might be categorized in one of three classes (light, medium, strong) and that value would concatenate with those of other parameters. Thus fuzziness would be eliminated altogether. To be effective, a large amount of parameters would be necessary to adequately control intraclass variance. Though this method is not replicated in later studies, its computational simplicity may tempt one to refine it until it attains acceptably low rates of error.

<u>Vielhauer et al. (2002)</u>

Vielhauer et al. designed a method for generating hash values from handwritten signatures. Their method produces a vector of 24 feature parameters. No reference samples were stored in the hashed template, an advantage that contrasted with variations of fuzzy cryptosystems which stored helper data.

Method

During enrollment, the user produces a signature on an acquisition device like a pen-based PDA. The coordinate signals x_t, y_t and the pen-up and pen-down signals p_{up}, p_t are collected from the supplied signature image. These three basic data form the basis of 24 feature parameters including, for example, the number of continuous pen-down sequences or the duration of the complete writing process in milliseconds. The values of these parameters are stored in an interval matrix IM such that

$$IM = \begin{bmatrix} \Delta I_1 & \Omega_1 \\ ... & ... \\ \Delta I_{24} & \Omega_{24} \end{bmatrix}$$

where ΔI_i is the interval length of an interval $[I_{Low} \ldots I_{High}]$ and $\grave{U}_i$ is the interval offset. ΔI_i is computed from initial intervals, such that

$$[I_{InitLow} \ldots I_{InitHigh}] = [\text{MIN}(n_{i,j}) \ldots \text{MAX}(n_{i,j})]$$

$$[I_{Low} \ldots I_{High}] = [I_{InitLow} * (1 - t_i) \ldots I_{InitHigh} * (1 + t_i)]$$

Where t_i is a tolerance factor derived from empirical tests of authentic writing samples against the above intervals and averaging the standard deviations. . ΔI_i and $\grave{U}_i$ can be expressed as

$\Delta I_i = I_{High} + 0.5 - (I_{Low} - 0.5) = I_{High} - I_{Low} + 1$

$$\Delta I_i = I_{High} + 0.5 - (I_{Low} - 0.5) = I_{High} - I_{Low} + 1$$

and

$$\grave{U}_i = I_{Low} \text{ mod}(\Delta I_i)$$

The hash values are calculated by mapping each feature parameter against IM . The hash function for each feature parameter f_i is written to a hash vector as such that

$$h_i(f_i, \Delta I_i, \Omega_i) = \left\lfloor \frac{(f_i - \Omega_i)}{\Delta I_i} \right\rfloor$$

Performance

The researchers achieved an average of 7.05% FRR at 0% FAR. These are impressive results compared to other methods reviewed that focus on the signature modality. The parametric approach to this method is similar to that of Hao et al. (2002); like theirs, this method is less complex than many of the other methods reviewed in this report and may be less expensive for systems to compute. The combined results of Hao et al. and Vielhauer et al. suggest that generating keys under the constraint of parameters could yield high security and robustness while maintaining computational simplicity.

Costanzo (2004)

Costanzo proposed a method by which biometric data was used to generate cryptographic keys suitable for use with symmetric cipher algorithms. He cited shortcomings in previous attempts,[76] claiming that their methods required prealigned inputs and expensive, complex computations. He intended for his method to surmount these shortcomings while producing keys that were highly entropic, unique, and stable.

Method

Costanzo's method adhered to the concept of adaptive boosting, wherein the aggregation of small classifiers is assumed to produce a more accurate classification than any single classifier. Classifiers and parameters are measured upon acquiring the biometric image. For example, a fingerprint image could be classified as having an arch with a parameterized ridge count between minutiae. This data would be used to generate a cryptographic key. The author did not go into detail on how to execute this process. Instead he proposed an idea wherein the greater the number of classifiers and parameters defined, the greater the number of total number of possible combinations (and thus entropy) of the key. If an algorithm is told to classify an input according to three distinguishing characteristics with two possible values each, the combination size would be six. This would yield 5,423,611,200 possible combinations on a 128-bit key, as calculated by

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} = \frac{P_{k,n}}{k!}$$

where n represents combination size and k represents key length.

Implications

The goal of this paper was to propose a simpler method for generating high entropy keys from biometric data. Its main contribution was the concept of encrypting a combination of parameter values derived from the input image, rather than encrypting the input image itself. Theoretically it would be much easier to replicate the exact same pattern of parameter values upon authentication than the exact same biometric image. Entropy would be guaranteed by defining more parameters, which yields more parameter combinations; while verification performance would be guaranteed by defining parameters easy to replicate despite fuzziness (e.g. whether a fingerprint is an arch or a whirl, rather than the exact coordinates of the minutiae).

Chen et al. (2009)

Chen et al. produced cryptographic keys from pseudo-signatures.[77] Such patterns are inherently cancelable, but they are easily susceptible to shoulder surfing in which someone observes the user during authentication and commits the pattern to memory. With this in mind, the researchers chose to extract behavioral data such as velocity and pressure in addition to the actual pattern during enrollment and authentication.

76

Monrose et al. (2001b), Clancy et al. (2003), Linnartz and Tuyls (2003).

[77] Pseudo-signatures are hand-drawn patterns used in the "Draw-a-Secret" graphical password scheme. They have been used to authenticate users in touchscreen smartphones.

Method

The proposed method reportedly follows that of Vielhauer et al. (2002) which processed a feature vector with an error correction algorithm to produce a cryptographic key. During enrollment, the user draws the same pseudo-signature m times to train the system. The training process assumes the following preliminaries:

$f_{i,j}$ is the feature value of the j"th" feature in the i"th" training sample;
$l_j'=\min(f_{i,j})$;
$r_j'=\max(f_{i,j})$;
$\Delta I_j=r_j'-l_j'+1$;
$l_j=l_j'-\Delta I_j \times \aa_j$; and
$r_j=r_j'-\Delta I_j \times \aa_j$ where $\aa$ is the tolerance value for the corresponding feature in a tolerance table.

The system constructs a feature vector from the training samples into an n×2 matrix $[(l_1,r_1),(l_2,r_2)\ldots(l_n,r_n)]$. A hash value of the feature vector is computed such that

$$H_j = \frac{f_{i,j} - \Omega_j}{\Delta I_j}$$

where i is the index of the training sample, and $\grave{U}_j=l_j \bmod (\Delta I_j)$ is auxiliary information representing the offset of the hashed feature. The feature space is divided into intervals along each dimension, allowing the system to map two inputs of negligible variation into the same output. The final output is a cryptographic key that is stored on the dataset. During authentication, the user draws a pseudo-signature to be compared against one or more secured templates in the dataset. The query is converted into a key using the same hash function employed during enrollment. If the difference in bits between the query and stored hash falls within a predefined threshold, the system returns a match and the user is authenticated.

Performance

The researchers tested the proposed method against offline, online, and trained attack models. They achieved 1% EER in the offline and trained attack models, and 4% EER in the online attack model. The researchers adapted their test methodology from a previous study which found that users drew more complex patterns when doing so on a background, rather than a blank canvas. With this in mind, they generate randomly patterned backgrounds on the canvas. The backgrounds do not actually affect the drawing; they merely encourage the user to draw more complex patterns. More complex patterns results in higher entropy templates.

4.9   Random Projection

Random projection is a means of reducing the dimensionality of a set of points while nearly preserving the distances between the points. The theory behind random projections stems from the Johnson-Lindenstrauss lemma, which

states that any set of k points in an n-dimensional Euclidian space can be embedded into an $O\left(\ln \frac{k}{\varepsilon^2}\right)$-dimensional space such that the pairwise distance of any two points is maintained to a reasonable extent.[78] Some template protection methods use random projection as a means to randomly map minutiae coordinates while preserving semantic meaning in final set.

4.9.1   Vulnerabilities

The irreversibility of a random projection matrix can be compromised if an attack can identify linkages among protected templates. This linkage can happen either where different protected templates are generated for different applications or where they are updated at different times. The attacker can exploit the leaked information either to reverse the genuine biometric feature vector or to filter out unlikely candidates for the genuine feature vector.[79]

---

[78] Johnson and Lindenstrauss, "Extension of Lipschizt Mapping into a Hilbert Space," 189-206.
[79] **Yang et al. (2010)**: 2.

Yang et al. (2010) mitigated this vulnerability by producing dynamic, nonlinear random projection matrices that make it difficult to launch inversion attacks in the event of a stolen token scenario. Wang and Plataniotis (2010) describe vulnerabilities that facilitate correlation attacks, cross matching attacks, and known projection attacks and means. [80]

4.9.2 Performance

Random projection methods have performed well in empirical tests. Chikkerur et al. (2008) and Yang et al. (2010) both exceeded the target of 1% FRR and 0.1% FAR.

4.9.3 Articles

Teoh et al. (2007)

Teoh and Yuang extended the BioHash method first proposed by Teoh et al. (2007). The original method was observed to distinguish genuine templates from imposters very poorly in the event that an imposter wielded a stolen token. They hypothesized that, in a stolen-token scenario, system performance would improve when using multispace random projections.

Method

The user submits a face image during enrollment. Facial features are extracted from the image and transformed into a feature vector x.[81] The vector is mapped onto a random projection vector v such that

$$v = \sqrt{(1/m)} Rx$$

where R is a random matrix m×n and n is the length of the biometric feature. The templates can be cancelled by issuing a new tokenized random number to the user.

Performance

The researchers tested the proposed method against 600 face images under normal conditions, a stolen-token attack scenario, and a stolen-biometric attack scenario. They also tested the methodology using two different feature extractors: EigenFace and Spectraface. Each test compared 718,800 imposter attempts and 3,600 genuine attempts. Under the stolen-token scenario, they achieved 31.23% EER with EigenFace as the feature extractor and 18.10% EER with Spectraface as the feature extractor.

Chikkerur et al. (2008)

Chikkerur et al. attempted to produce cancelable fingerprint templates without requiring prealignment of the minutiae points. Their goal was to build a more robust system that could withstand image registration errors, without compromising security in the template design. They criticized the inability of biometric cryptosystems[82] to withstand intraclass variation adequately. They determined that geometric registration may not be required for the construction of cancelable templates, which they observed to be commonly used in fingerprint recognition. Instead they used purely local measurements.

Method

---

[80] Wang and Plataniotis, 2010, "An Analysis of Random Projection for Changeable and Privacy-Preserving Biometric Verification," 1287.

[81] The feature extraction process is not investigated in this article.

[82] See, e.g., Monrose et al. 2001; Teoh et al. 2004.

For each transaction the user presents a fingerprint image to an acquisition device. An image patch is extracted from each minutiae point rather than its coordinates. The patches were aligned with the angle of the minutiae to ensure accurate matching performance. To calculate the similarity among the patches, a normalized dot product function computes the distance d between a query template x and a stored template y such that

$$d(x,y) = 1 - \frac{x^T y}{|x||y|}$$

Ultimately the expansion coefficients, derived from a Gabor basis expansion of the patches, form a unique signature to be stored in the dataset. The noninvertible, cancelable transform T is executed such that

$$T(x, B_k) = sgn(B_k^T x)$$

where B_k^T is a user specific projection matrix.

During authentication, the user presents a fingerprint image. A signature is generated from the features in the same way that is done during enrollment. A similarity score S between the query signature $\{x_i\}$ and a stored signature $\{y_i\}$ is computed such that

$$S(\{x_i\}, \{y_i\}) = \frac{\sum_{\min(M,N)} \left(s(x_i, y_{T(i)}) \right)^2}{M \times N}$$

where T(i) is the index of the minutiae in set $\{y_i\}$ to that in set $\{x_i\}$.

Performance

Having tested the proposed method against 17,578 imposter comparisons and 188 genuine comparisons, the researchers achieved as low as 0% FRR at 0.1% FAR when the cancelable transform was employed. False acceptance rate was much higher when the cancelable transform was not employed.

Al-Assam et al. (2009)

Al-Assam et al. designed a method for producing cancelable biometric templates using noninvertible, random projection transforms, an approach also attempted by Teoh et al. (2004). They claimed that the method could match or exceed the verification performance of existing methods using random projections. Their explicit goals were to create templates that were resistant to cross matching, highly entropic and noninvertible, cancelable, and negligibly detrimental to verification performance.

Method

Random projection maps data from orthonomal matrices to other spaces and preserves the distances among the data points. The researchers observed previous random projection methods to have three steps: (1) to generate m pseudorandom vectors from a user key or token; (2) to apply the Gram-Schmidt algorithm[83] to convert the vectors into orthonomal matrices, which have the same dimensionality as the original template feature n; and (3) to transform the original template feature x to a secure domain using a matrix product y=Ax. They claimed that small orthonomal matrices could be generated without using the Gram-Schmitd algorithm.

Their modified approach, which they reported to be computationally more efficient, had just two steps. First they selected a set of n random values {$_1$, $_2$... $_n$} in the range [0...2] according to a user key or token to create an orthonomal matrix A. Then they transform the original biometric template from a secure domain y=Ax. They noted

---

[83] See pp. 3-4 for an overview of the Gram-Schmitd algorithm.

that, in practice, they would apply a secret permutation such that y=Ax+b where b is a blinding vector.

Performance

The researchers tested the proposed method against two datasets: one with 165 face images, the other with 80 face images. They used wavelet decomposition to achieve face recognition and nearest neighbor classification to achieve matching. When using no transformation, they achieved 21% EER and 17% EER from the respective datasets. When using their proposed method, they achieved 2% EER and 0.2% EER respectively. This method could potentially match the verification performance of preceding methods using random projection.

Ouda et al. (2010)

Ouda et al. recognized that even though BioHash[84] and other token-based methods for cancelable biometrics yielded the most accurate match rates, their resistance to stolen-token attacks was weak. Therefore they proposed a method of producing cancelable templates in such a way that did not require tokens but could still compete with token-based methods in terms of matching performance. They proposed a single-factor authentication scheme called BioEncoding.

Method

For each transaction, the user presents an iris image from which its features are extracted to form an IrisCode. To reduce noise, consistent bits[85] are selected from the extracted template. To this end they first aligned the query template with the stored template, which the researchers achieved by rotating the query image by r-degree intervals until the features reach an angle that minimizes the Hamming distance. Then they masked the bits that were likely to be the same value at similar locations in both templates, omitting those with high variability. The consistent bits were stored in a vector C. The researchers claimed that consistent bit extraction was an important step in optimizing verification performance.

The final template, called a BioCode, is generated from the consistent bits and scrambled into a compact string.[86] Prior to enrolling users the server stores a random seed that generates a pseudorandom sequence of length 2^m that is used to randomly map the consistent bits. Cancelling a BioCode is simply a matter of changing the value of this random seed. And while the researchers correctly assume that one random seed would suffice for all users in the system, it would be preferable for each user to have a unique random seed so that one could cancel and reenroll her template without requiring all other users to reenroll their templates. For each transaction, the consistent bits of the feature vector are first grouped into n address words of m length. Each address word in C is mapped to the bit value in S where the position is addressed by the value in that word. An example is given where an address word 111101, which is equal to the decimal 61, is mapped to 0 or 1 depending on whether the value at position 61 in the pseudorandom sequence is 0 or 1. To authenticate a user, the entire process is repeated and the query BioCode is compared against one or more stored BioCodes.

Performance

The researchers tested the proposed method and the BioHash method against 756 iris images from the CASIA dataset. They found that, on average, one in five bits were perfectly consistent among all IrisCodes. After 566,244 imposter comparisons and 756 genuine comparisons, they found that BioCodes produced 1.3-2.1% EER while BioHash produced 2.2-5.8% EER. But the proposed method has some scalability issues. The more trivial issue is the need to submit multiple images during enrollment in order to train the system. The greater issue is that the random seed is shared among all users enrolled in the application. To cancel one user requires reenrolling all users, which would be impractical for to execute in large scale applications.

---

[84] See **Teoh et al. (2004)**.
[85] "Reliable" or "consistent" bits have a high probability of having the same value in the same areas among multiple images of the same iris.
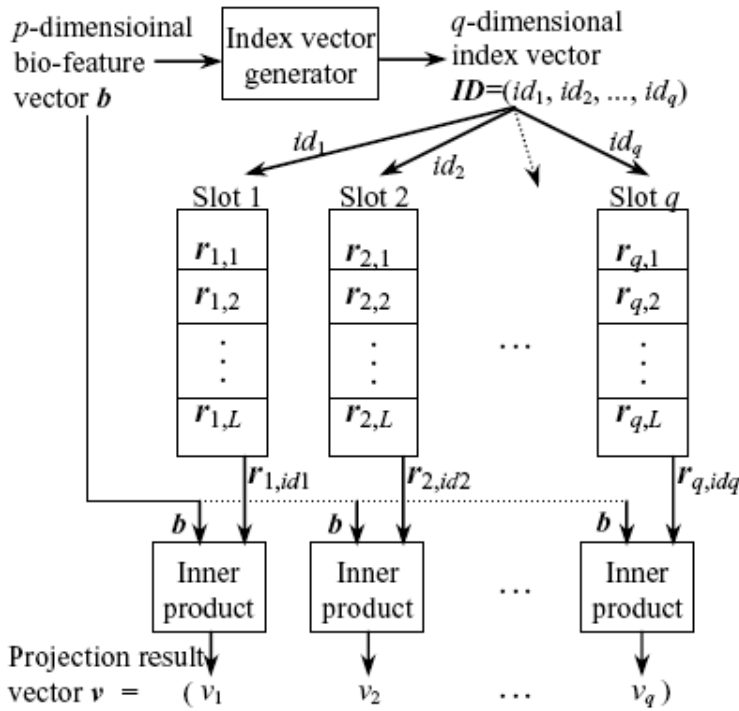[86] See pp. 6-7 for diagrams of BioCode generation.

Yang et al. (2010)

Figure 30: Schematic overview of the anonymous biometric access control system.

Yang et al. designed a new approach to random projection for biometric template protection in reaction to the security concerns of the stolen-token scenario as explained by Teoh et al. (2007). The concerning issues, the researchers noted, was that the matrix was both public and linear. The proposed method dynamically constructs a nonlinear random projection matrix instead of a fixed random projection matrix, increasing the computation complexity of reverse engineering a secured biometric template. The proposed method performed very well in empirical tests. This research was funded under Project TURBINE (ICT-2007-216339).

Method

Figure 30 illustrates a high level overview of the proposed system. To dynamically construct a random projection matrix, q random vector slots are set to be public with each slot i containing L p-dimensional random vectors. From each slot, one of the L random vectors is selected for projecting the biometric feature vector b to obtain one dimension of the projected result vector v. The selection of $r_{i,j}$ will be decided by an index id_i is which is the jth dimension of an index vector $ID=(id_1,id_2…id_q)$ such that with all the public slots there is no clue to the attacker which random vector $r_{i,j}$ from the slot i was selected to as $r_{i,idi}$ to project b into the ith dimension of v:

$$v_i=(r_i,id_i) b$$

An index vector generator function can be designed to take the biometric feature vector b as the input and output the q-dimentional integer index vector ID. This new mechanism makes the creation of the projection matrix dependent on the to-be-projected biometric feature vector. The researchers presented two amplitude quantization functions: one to be applied to the biometric feature vector, the other to be applied to a fixed-matrix based random projection result vector.[87]

Performance

The researchers tested the proposed method against 800 fingerprint images in the stolen token scenario. They achieved 0.6% FRR at 0.1% FRR meeting at 0.57% EER where the length of the secure binary string was 144 bits. These are among the most promising results of the tests reviewed in this report. These results were achieved when the input images were not manually prealigned.

---

[87] See p.3 for details on the amplitude quantization functions.

5 Iris Recognition Assessments and Performance Evaluations

5.1 Background

Iris recognition technology is considered a candidate for use in biometric PETs due to the richness and stability of data in iris images. To gauge the suitability of this modality for use in PETs, Indiana University-Purdue University Indianapolis (IUPUI) analyzed previous studies of iris recognition performance and conducted a new study of iris recognition performance. References for this section are marked in brackets and are listed in Annex G.

5.2 Assessment of Iris Recognition through Variable-Quality Iris Datasets

5.2.1 Test Iris Image Datasets

Iris image quality is likely to be a determinant of the viability of such use. To this end, IUPUI evaluated the ability of a commercial iris recognition algorithm to process seven iris image datasets of varying quality. Representative images from each dataset are shown in Figure 31.

Dataset Name	Image Format & Volume	Quality / Capture Notes
Iris Challenge Evaluation (ICE)	640x480 , 2953 images	Controlled environment, cooperative subjects, illuminated in the near infra-red (NIR) range
Chinese Academy of Sciences (CASIA) 2.0	640x480 , 2400 images	NIR
CASIA 3.0 Set 1	320x280 , 2639 images	NIR; captured in two sessions, at least one month interval
CASIA 3.0 Set 2	640x480 , 16213 images	NIR; captured in one session
CASIA 3.0 Set 3	640x480 , 3183 images	NIR; captured in one session
West Virginia University	640x480 , 1852 images	NIR; noisy, heterogeneous data, with obstructions, inconsistent illumination, and out-of-focused, off-angle irises
UBIRIS	800x600 , 1877 images	Color images acquired in visible wavelengths; Two distinct sessions, images are predominately frontal gaze,
Multimodal Biometric Grand Challenge (MBGC)	2048x2048 , 148 videos, 1 second duration	NIR; focal length of IOM is 2~3 feet, images acquired while subjects walked toward the camera, primarily frontal view, human subjects are instructed to look at iris cameras
IUPUI multi-wavelength	1280x1024 , 352 videos	NIR; obtained from both eyes on two separate occasions, time period between each data acquisition is at least one week, only used green wavelength to test
IUPUI Remote	1280x1024 , 731 videos, 30 fps	NIR; average iris radius was 95 pixels, data was acquired in two sessions, at least one week between sessions, 6 videos per iris, variety of positions and situations

Iris Challenge Evaluation (ICE) images are 640x480 resolution and illuminated in the near infra-red (NIR) range, acquired using the LG IrisAccess 2200. The dataset contains 2953 images (1426 left eyes and 1527 right eyes). Acquisition was performed in a controlled environment with cooperative subjects.

CASIA iris datasets were created by the Institute of Automation from the **Chinese Academy of Sciences (CASIA)**. CASIA ver. 2.0 includes 2400 images (640x480) of 60 eyes. CASIA 3.0 is comprised of 3 different sets. Set 1 contains 249 subjects, 385 classes, and 2639 images (320x280). Most images were captured in two sessions, with at least one month interval. Set 2 contains 411 subjects, 819 classes, and 16213 images (640x480). Set 3 contains 200 subjects, 400 classes, and 3183 images (640x480) from 100 pairs of twins. Both second and third sets are one session.

The WVU Dataset, consisting of 1852 images (640x480) of 380 eyes, was developed by the **West Virginia University**. WVU images were captured with few environmental constraints, resulting in noisy, heterogeneous data, with obstructions, inconsistent illumination, and out-of-focused, off-angle irises.

The **UBIRIS** dataset images are color images acquired in visible wavelengths, in comparison to most iris datasets which are acquired using NIR. The dataset consists of 1877 images (800x600) composed of 241 users in two distinct sessions. The images are predominately frontal gaze.

The **Multimodal Biometric Grand Challenge (MBGC)** NIR video dataset was acquired using Sarnoff's IOM system. It consists of 148 one-second videos (2048x2048) from 114 subjects. The focal length of IOM is about 2~3 feet. Images are acquired while subjects walk toward the camera. These video images are primarily frontal looking iris images and the human subjects are instructed to look at the iris cameras.

The **IUPUI** multi-wavelength dataset was acquired under eight different wavelengths illumination including Purple (420 nm), Blue (470 nm), Green (525 nm), Yellow (590 nm), Orange (610 nm), Red (630 nm), Deep Red (660 nm), and Infra-Red (820nm) at a distance of one foot. In each wavelength, there are total 352 images of 44 subjects whose eye colors included blue, dark brown, light brown, green, and hazel. For each human subject, we obtained the image videos (1280x1024) from both eyes on two separate occasions. The time period between each data acquisition is at least one week. In this experiment we only used the Green wavelength to test.

The **IUPUI remote** non-cooperative dataset included, for each eye at each session, 6 iris videos.

- The first video was frontal and the eye was still.
- The second and third videos were captured while subjects read sentences from wall-mounted posters (placed 15 feet away from the subject, about 5 feet behind the camera)
- The fourth and fifth videos were acquired while the subjects were searching the wall to calculate the total number of certain symbols
- The sixth video was acquired while subjects did simple numerical calculations with the numbers placed on the ceiling of the room.

Each 1280X1024 video was captured at 30 frames per second. The average iris radius of the video images in the dataset was approximately 95 pixels. Each subject's data was acquired in two sessions, with at least one week between sessions. The dataset consists of 31 subjects, 62 irises, 731 iris video sequences, and 205,538 video frames.
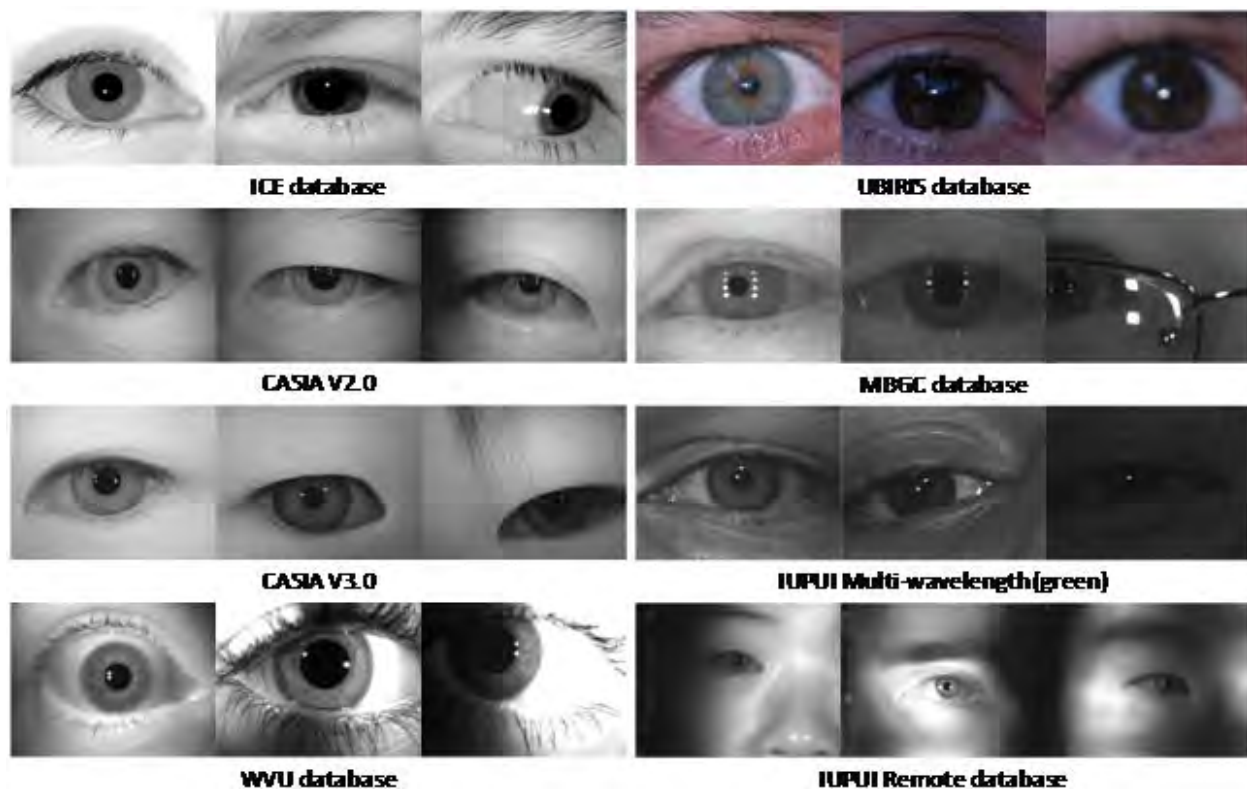
Figure 31: Representative Iris Images

5.2.2 Performance Evaluation Metrics

Metrics used to evaluate performance were false rejection rate (FRR), false acceptance rate (FAR), and failure to process rate (FTPR). These statistics are based on the following matching outcomes [62]. True Negatives (TN) are different-iris pairs correctly identified as being from different eyes. False Positives (FP) are different-iris pairs incorrectly identified as the same eye. False Negatives (FN) are same-iris pairs incorrectly identified as not being the same iris. True Positives (TP) are same-iris pairs identified as the same iris.

FRR is calculated as:

$$FRR = \frac{FN}{TP + FN} * 100\% \qquad . (2\text{-}1)$$

FAR is calculated as:

$$FAR = \frac{FP}{TN + FP} * 100\% \qquad . (2\text{-}2)$$

FTPR is calculated as:

$$FTPR = \frac{\text{\# of Images that failed to process}}{\text{Total \# of Images}} * 100\% \qquad . (2\text{-}3)$$

5.2.3 Results and Analysis

Summary quality results are shown in Figure 32. Images that failed to process were given a score of 0.
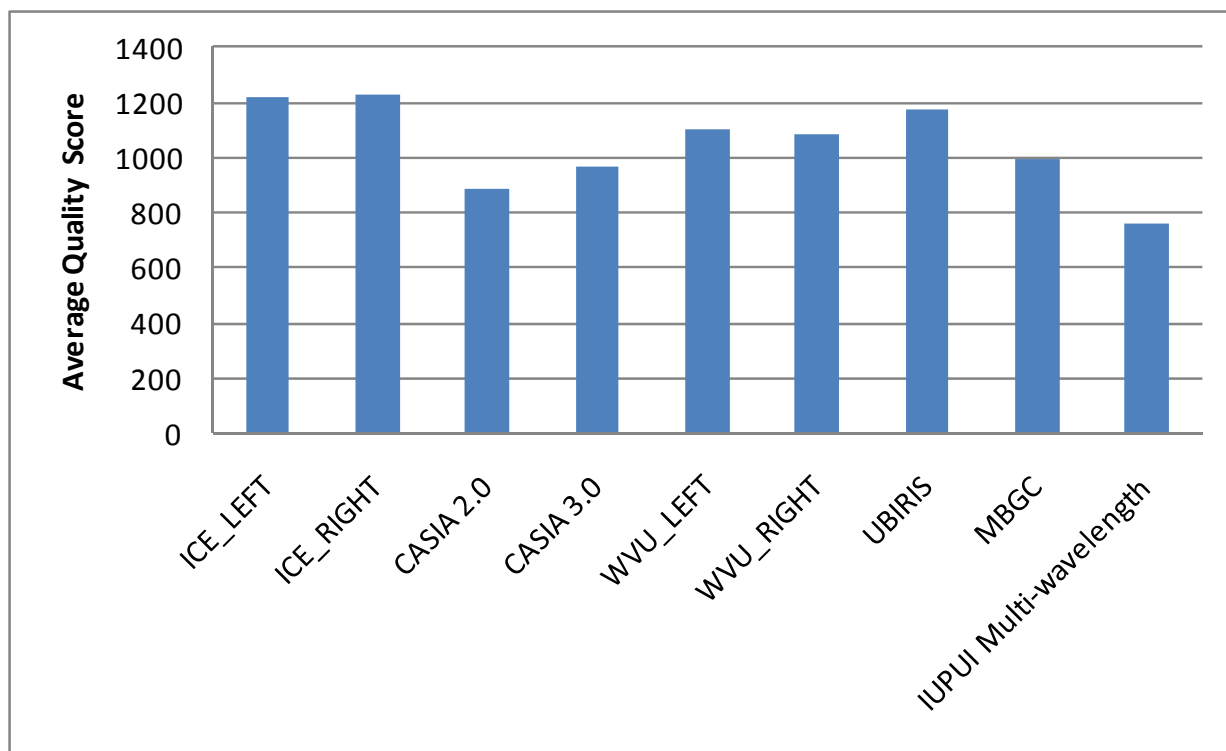
Figure 32: Quality score of all datasets

Summary processing and matching results are shown in Figure 33.

Dataset	# of Images	# of Eyes	FTPR	FRR*	FAR*
ICERIGHT	1528	120	0%	5.47%	3.05×10^{-4}%
ICELEFT	1425	124	0.07%	3.91%	1.49×10^{-4}%
CASIA 2.0	1200	60	2.75%	20.63%	0
CASIA 3.0	3183	400	2.8%	23.05%	5.94×10^{-5}%
WVULEFT	1562	190	1.22%	15.16%	0
WVURIGHT	1537	234	0.85%	13.3%	1.28×10^{-4}%
UBIRIS (part 1)	1214	241	0.58%	12.5%	5.45×10^{-4}%
MBGC	1072	285	4.57%	38.28%**	1.75×10^{-4}%
IUPUI MULTIWAVE	886	88	19.07%	41.69%***	4.67×10^{-3}%
IUPUI Remote	731 videos, 205,538 images	62	NA	NA	NA

Figure 33: Summary of Iris Recognition Performance for Test Datasets

Results are shown in chart form in Figure 34 and Figure 35.

Figure 34: Comparative Failure to Process Rates

Figure 35: Comparative Accuracy Rates

FRR and FAR were based on a Hamming distance of 0.33 as threshold (the default setting). By comparison, in [1] Daugman suggested that a Hamming distance of 0.26 would result in a zero FAR in a large dataset. A Hamming

distance of 0.26 would have a higher FRR.

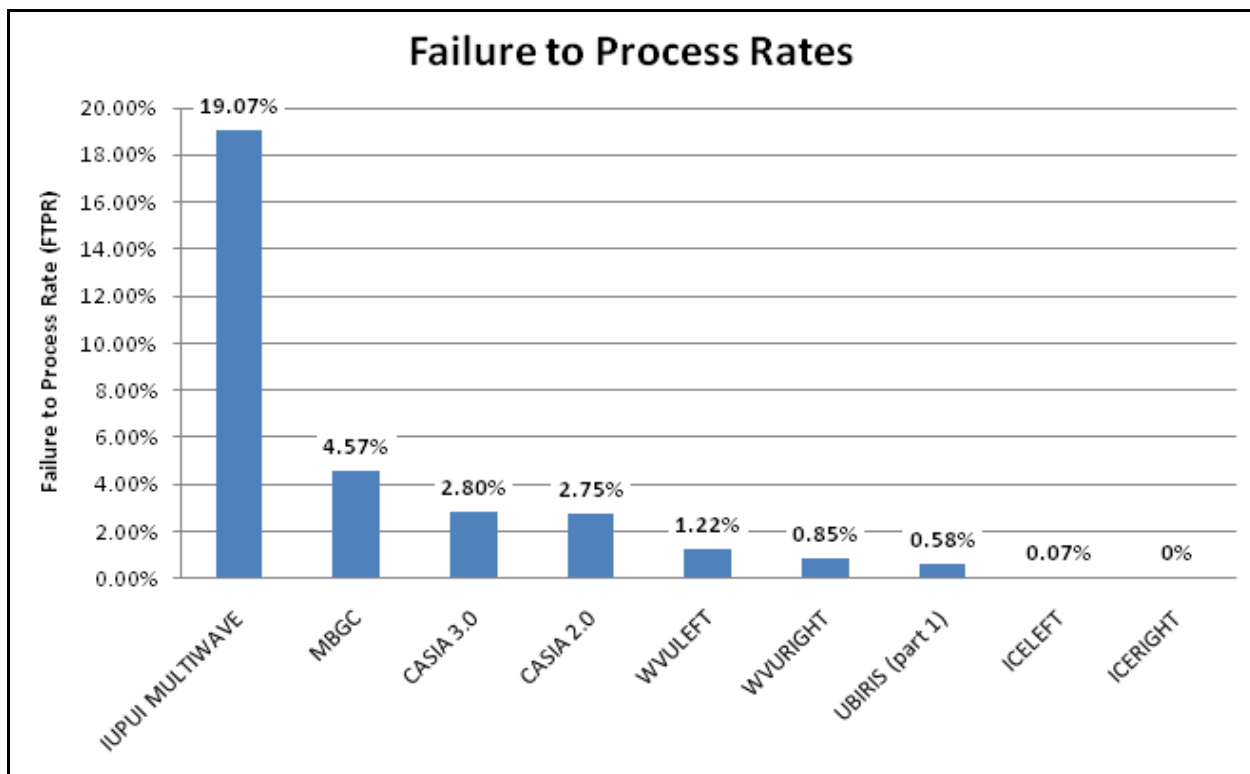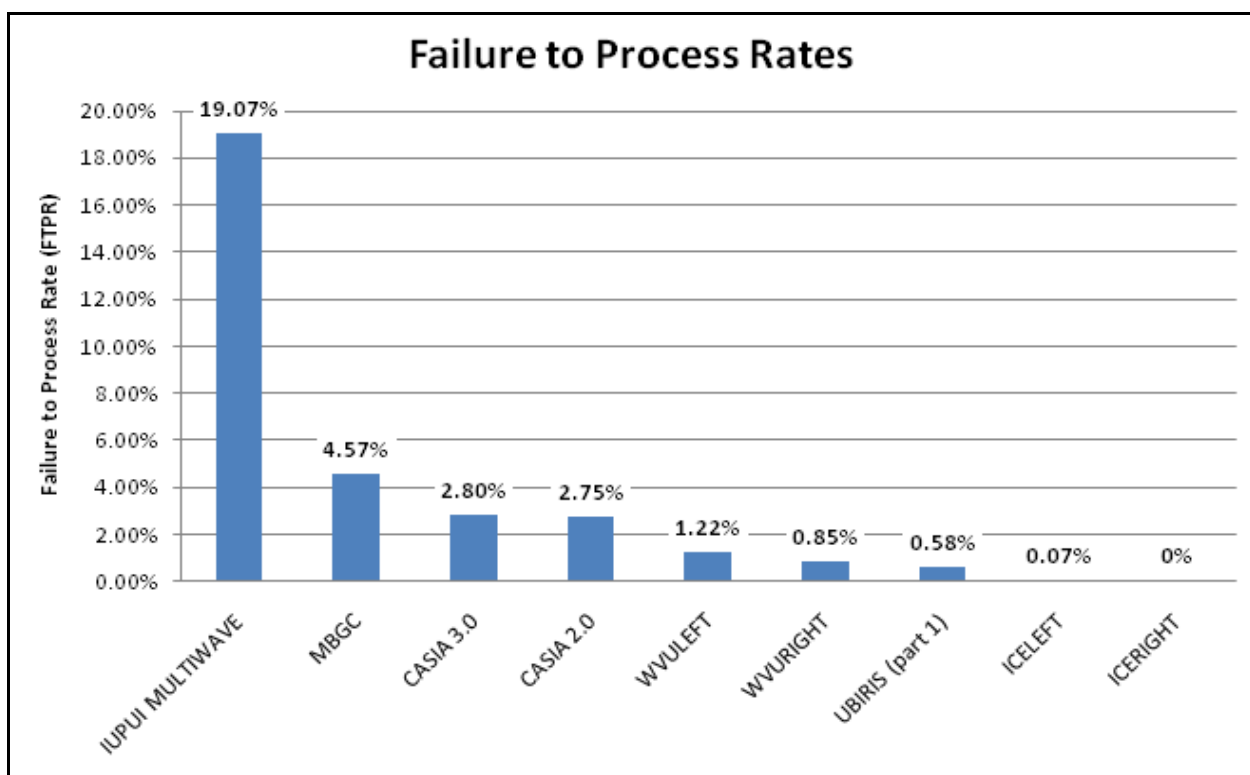The resolution of the iris patterns in the MBGC dataset are about 150 pixels across the iris, which is much lower than the expected working environment of the commercialized system. This accounts, in whole or part, for the FRR (38.28%) for this dataset. Because iris patterns in dark brown eyes are hard to be extracted in visible wavelengths, the FRR in IUPUI dataset is high (41.69%).

The ICE dataset [63] has high accuracy and quality. Its images were acquired using a commercial NIR iris camera under well controlled environment with good illumination. The overall recognition accuracy for this dataset is high with very low FRR and FTPR. A small number of bad quality images with high occlusion were falsely rejected. In addition, one off-angle image in the ICE dataset has greatly affected the accuracy as Daugman has analyzed in [25]. There is a very small FAR. The lowest Hamming distance of false accepted pair is 0.3083.

The CASIA datasets [64] had relatively low quality. Most human subjects for this dataset are Asians whose eyes sometimes are small and eye lashes often occludes iris patterns. The FRR is relatively high, as many images have been rejected due to heavy occlusion. The smallest false acceptance Hamming distance for this dataset is 0.3218.

The WVU dataset's [65] illumination is less consistent than the system expects, dramatically affecting its accuracy. Some images even have iris completely covered in a shadow. 0.3173 is the smallest false acceptance Hamming distance for this dataset.

UBIRIS [39] is a color iris dataset. Although the commercial system is designed to work on NIR images, it performed surprisingly well in this dataset. Some images are falsely rejected because the irises are too dark to be viewed in the visible wavelengths. In addition, some images are very blurry. 0.3149 is the smallest false acceptance hamming distance in this dataset.

MBGC dataset [66] didn't perform well, as the commercial iris recognition algorithm used in the evaluation is designed to perform iris recognition using NIR face images. Extracted irises were approximately 150 pixels in diameter, much lower than the expected working environment of the commercialized system. In addition, some irises are not fully contained in the image, and one image shown in Figure 31 is even partially covered by eye glasses. This explains the dataset's high FRR and FTPR. It is reported in Matey's paper [5], that with proper segmentation, Daugman's recognition method can work very well in MBGC dataset. IOM systems are capable of adequate performance using MBGC-style images.

The IUPUI multispectral dataset has very high resolution images and had to be downsized to work in the system. The downsizing process could distort the iris patterns, which could account for the high FRR. Since we used the images from green, yellow, and NIR wavelengths, some dark brown iris images are too dark to be used for recognition, potentially contributing to high FRR. Even though there are several false matches, 0.3151 is the smallest false acceptance Hamming distance in this dataset. As anticipated, the test system was unable to process the IUPUI Remote dataset due to the low resolution and non-frontal capture of its images.

Cross-matching of iris images from different datasets did not result in any false matches.

The following conclusions can be drawn from this multi-dataset evaluation of a commercial iris recognition system:

- Processing and matching are very fast. The system can perform iris recognition in 17.8ms (including segmentation, feature extraction and 1:1 matching).
- It has very low FAR when using a decision threshold (Hamming Distance) of 0.33. As Daugman has discussed in [1], for large-scale matching, the recommended HD is 0.26. Such a threshold would have resulted in a 0.00% FAR and higher FRR for all datasets.
- The system is capable of processing visible wavelength images, assuming that iris patterns are good enough for recognition.
- The system can work reasonably well with regular pupil dilation.
- The system is designed to reject poor quality images to avoid possible false acceptance.

Areas for improvement include the following:

- The system is unable to process non-cooperative, off-angle iris images.
- Since the commercialized system is designed for images acquired from a specific, paired acquisition system, preferences in iris image resolution and illumination are present. Usually, the commercialized system can work best with iris images with resolution about 200 pixels across the iris. However, for lower resolution or higher resolution images, if resolution can be adjusted properly without deforming iris patterns, the system can also perform accurate iris recognition.
- Recognition accuracy can be affected dramatically by poor illumination condition or poor contrast.
- Recognition accuracy can be affected dramatically by motion blur.
- The commercialized system would not work with dark color iris images in visible wavelength due to the lack of recognizable iris patterns.
- Hamming Distances are not necessarily symmetric. When used for enrollment, lower-quality images resulted in higher (worse) HDs.

5.3 Impact of Compression on Iris Recognition

5.3.1 Background

The goal in the section is to study how the state-of-the art iris recognition system performs when the image of the iris has been compressed. There are two topics in iris image compression: the consequences of iris pattern compression to the iris recognition accuracy and how to achieve the highest possible compression without compromising iris recognition accuracy. In this section, we first study how iris pattern compression would affect iris recognition accuracy and how to measure image quality. Then we examined how to achieve high compression rate which is possible by reserving as much information as possible in the iris pattern area.

Data compression is beginning to play a part in the use of iris recognition systems. In the field applications using handheld iris recognition devices often use wireless communication to connect to the central server for identification and verification. Law enforcement agencies, such as the Border Patrol, the Coast Guard, and the Armed Forces, are using portable wireless iris recognition devices. While it will be ideal to have wide bandwidth for transmission in real-life applications, it often needs to transmit captured images or templates over a narrow-bandwidth communication channel. In this case, minimizing the amount of data to transmit (which is possible through compression) minimizes the time to transmit, and saves energy. There are other iris applications that require a full-resolution iris image to be carried on a smart card, but require a small fixed data storage size. In some cases (such as surveillance applications), the images acquired have already been compressed. If the image has been compressed it is important to know how much it has been compressed and to what degree the compression will affect the recognition accuracy.

5.3.2 Compression and Iris Recognition Accuracy

Ives et. al. [67] and Du et. al [46] studied how compression in iris images would affect compression accuracy. JPEG 2000 was used on the ICE dataset [68]. JPEG 2000 is a state of the art compression method; it uses a discrete wavelet transform to compress an image. JPEG 2000 is published by the Joint Photographic Experts Group. For this paper the default parameters and options of the JasPer implantation of JPEG 2000 were used [69]. In this way the compression rate was uniform across the entire image and no special priority was given to the iris area.
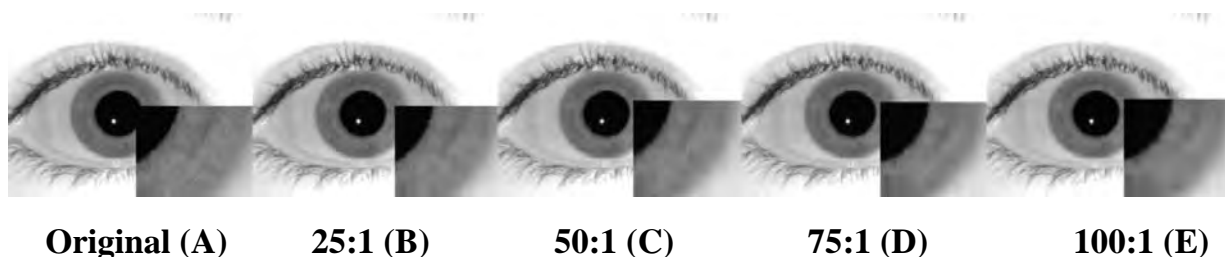

| Original (A) | 25:1 (B) | 50:1 (C) | 75:1 (D) | 100:1 (E) |

Figure 36: Sample image at various levels of compression [67]..

Figure 36 shows the original image and 4 different compression rates. As the compression is increased some of the finer details get lost and artificial patterns get introduced into the image. Both of these factors will affect image quality and recognition accuracy.

Compared Databases	Minimum HD	Mean HD	Maximum HD
Original versus Original	0.0025	0.1535	0.4795
Original versus 25:1	0.0000	0.1514	0.4818
Original versus 50:1	0.0000	0.1685	0.4705
Original versus 75:1	0.0008	0.1912	0.4742
Original versus 100:1	0.0035	0.2109	0.4802

Figure 37: Summary of Iris Recognition Performance for Test Datasets

Figure 37 shows the genuine match results at various levels of compression. Lower HD means the images are a better genuine match. The data consists of 2953 images, 1425 were right eyes of 124 different people and 1528 were left eyes from 120 different people. There is a slight improvement in Hamming distance in the min and the max for the first three levels of compression and there is an improvement for the first level of compression for the mean. It is expected that the Hamming distance would increase as the compression increased because data is lost and the genuine matches become less similar. The decrease in Hamming distance is probably because the compression removed some noise and/or in the small data set an artificial patterns appeared that was unique for a particular iris.
.

	EER (%)				
	Original	Cr25	Cr50	Cr75	Cr100
Original	1.350	1.470	1.540	2.020	2.500
Cr25	1.470	1.730	1.770	2.280	2.800
Cr50	1.540	1.770	2.010	2.420	3.000
Cr75	2.020	2.280	2.420	3.010	3.350
Cr100	2.500	2.800	3.000	3.350	4.450

Figure 38: Iris Recognition Cross-Matching EER

Above are cross-matching results Figure 38 is equal error rate, in this table the EER increases as the compression increase. This shows that the compression decreases the accuracy.

	FRR at FAR = 0.001				
	Original	Cr25	Cr50	Cr75	Cr100
Original	0.022	0.024	0.028	0.042	0.057
Cr25	0.024	0.030	0.035	0.049	0.069
Cr50	0.028	0.035	0.044	0.057	0.075
Cr75	0.042	0.049	0.057	0.079	0.088
Cr100	0.057	0.069	0.075	0.088	0.125

Figure 39: Iris Recognition FRR at FAR= 0.001.

Figure 39 is false rejection rate at false acceptance rate=0.001, this table shows a decrease in FRR every time that

compression is increased.

| FRR at FAR = 0.0001 | | | | |
	Original	Cr25	Cr50	Cr75	Cr100
Original	0.036	0.043	0.060	0.087	0.106
Cr25	0.043	0.070	0.088	0.126	0.149
Cr50	0.060	0.088	0.105	0.134	0.153
Cr75	0.087	0.126	0.134	0.177	0.170
Cr100	0.106	0.149	0.153	0.170	0.223

Figure 40: Iris Recognition FRR at FAR = 0.0001.

Figure 40 is false rejection rate at false acceptance at 0.0001. This table shows a decrease in FRR as compression increase in all but one instance. The 100:1 compression image compared to the 75:1 image preformed worst than the 75:1 compared to the 75:1. The FRR is very close 0.177 for the 75:1 to 75:1 and 0.170 for the 100:1 to 75:1. This result is likely a statistical anomaly because it was very small and it only occurred in this one test. These tables also show that mean HD shouldn't be the only measure used to evaluate the quality of an image because these tables show that accuracy is greatly impacted by compression.

5.3.3 Compression and Iris Image Quality

Poor quality image can affect recognition accuracy because they do not have enough feature information. In [70], we proposed the feature correlation evaluation based method to measure image quality. By using information as a measure, it can not only describe the randomness of the features, but also generate high-order statistics of the iris image based on its features [70]. For compressed images, the artificial patterns introduced by the compression generally would be more correlated than the natural iris patterns. That means there would be less difference between adjacent artificial patterns. Using information distance as a measure, we can measure the feature quality. The combination of occlusion and dilation determines the amount of iris patterns available in matching, and is also considered in the proposed quality measure.

Figure 41 shows the feature correlation measure score for each row of the eye in Figure 36. A is the normal image, B is the 25:1 compression, C is 50:1 compression, D is 75:1 compression, E is 100:1 compression. It shows that the FCM decreases as the compression increases. This shows that feature information is reduced with increasing of compression, which results in lower image quality. The quality scores for (A) to (E) are 0.9975, 0.3784, 0.2660, 0.2539 and 0.2008 respectively.
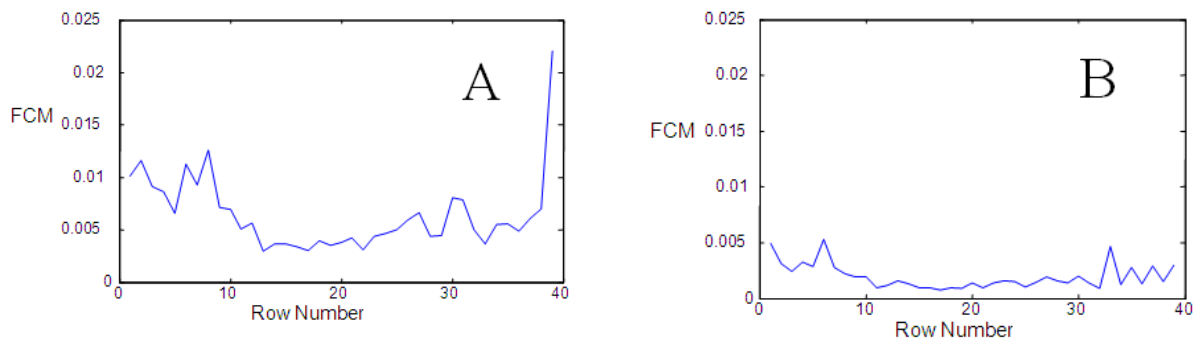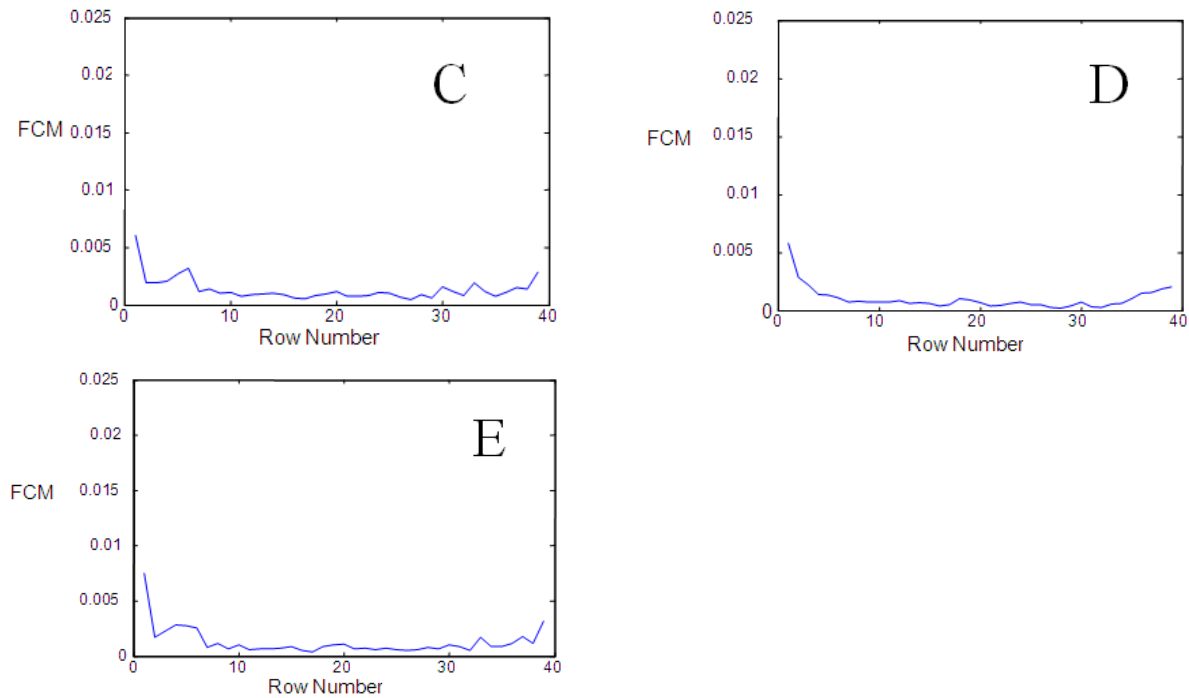
Figure 41: Row-by-row feature correlation

Figure 42 shows the mean quality score decreases with increasing of compression rate. The rate of decrease is greater at lower levels of compression. This means that the rate of information lose is greatest for the first stages of compression.
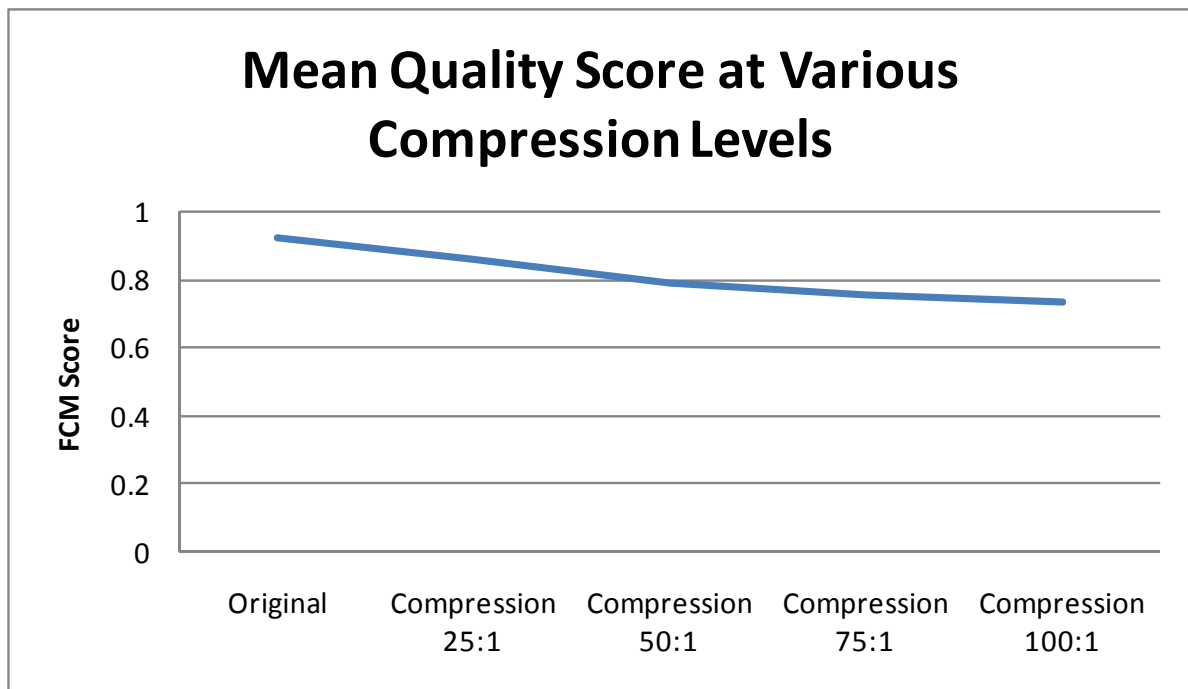

Figure 42: Mean quality score at various compression levels

5.3.4 Region of Interest Compression

A regular image compression scheme could affect iris recognition accuracy and iris image quality significantly. In [71], Daugman designed a Region of Interest based iris compression method to achieve better compression rate. Figure 43 shows the diagram of Daugma's compression approach. It first detects the iris area and crop the images to reduce size. Next the eyelid and eyelashes are replaced with a gray area to take less space when the image is compressed. Finally the image is compressed using Region of Interest (ROI) approach. See Figure 44 for examples.

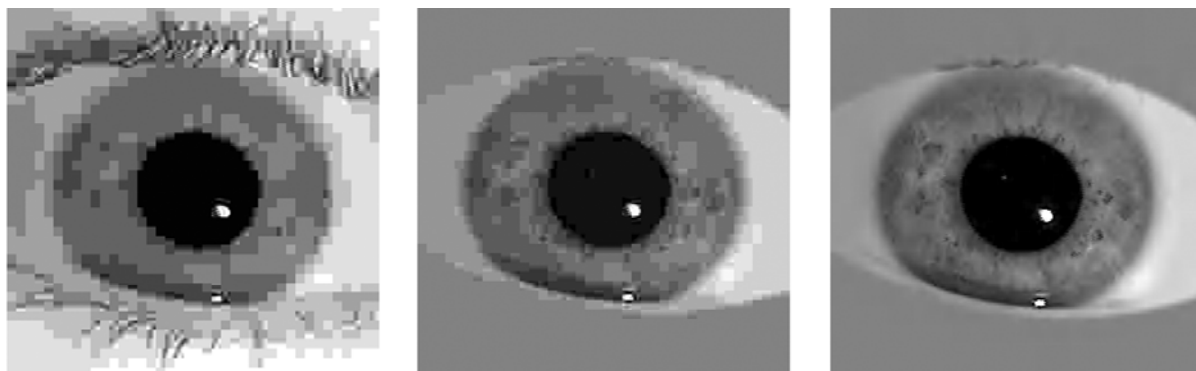Figure 43: The diagram of Daugman's compression approach ..

Figure 44: *From left: JPEG compressed, Isolated JPEG, and JPEG2000*[71]

For ROI-based approach, there JPEG and JPEG 2000. JPEG 2000 is designed to allow for a region of interest to be assigned and in that way the JPEG 2000 compresses the image in such a way that it preserves more of the data in the ROI. Figure 45 shows the comparison of the Hamming distance using ICE dataset left eyes (1425 images from 124 individuals). The total compression is calculated by dividing the original image size 640x480 or 307.2 KB by the average image size after compression using Table 1 in Ref. [71]. The compression parameter QF means quality factor CF means compression factor. HD means Hamming Distance. The greater increment of Hamming Distance means more reduction in recognition accuracy.

Figure 46 illustrates the compression rate vs hamming distance increase using Table 1 from[71]. These results are similar to the findings in [67] that show as compression increases the Hamming distance increases. Using cropping, RIO and JPEG 2000, the system can achieve 153.6:1 with only increasing the Hamming distance to 0.027. And, it has been shown it is possible to compress an iris image 180:1 with an increase in hamming distance of only 0.035. An increase in Hamming distance of 0.02 to 0.03 is negligible[71] and this show that it possible to compress an image greatly but still preserve the iris information if the image is compressed after the iris is detected and segmented. On the other hand if the image is compressed before segmentation a 100:1 compression ratio results in a greater increase in hamming distance. The increase in hamming distance is 0.057 between the original to original and the 100:1 to original. This shows it is possible to store an iris image in a small format if it can be segmented first, but using an iris image that comes from an extremely compressed source is more difficult, because the background and iris are given the same priority when image was compressed.
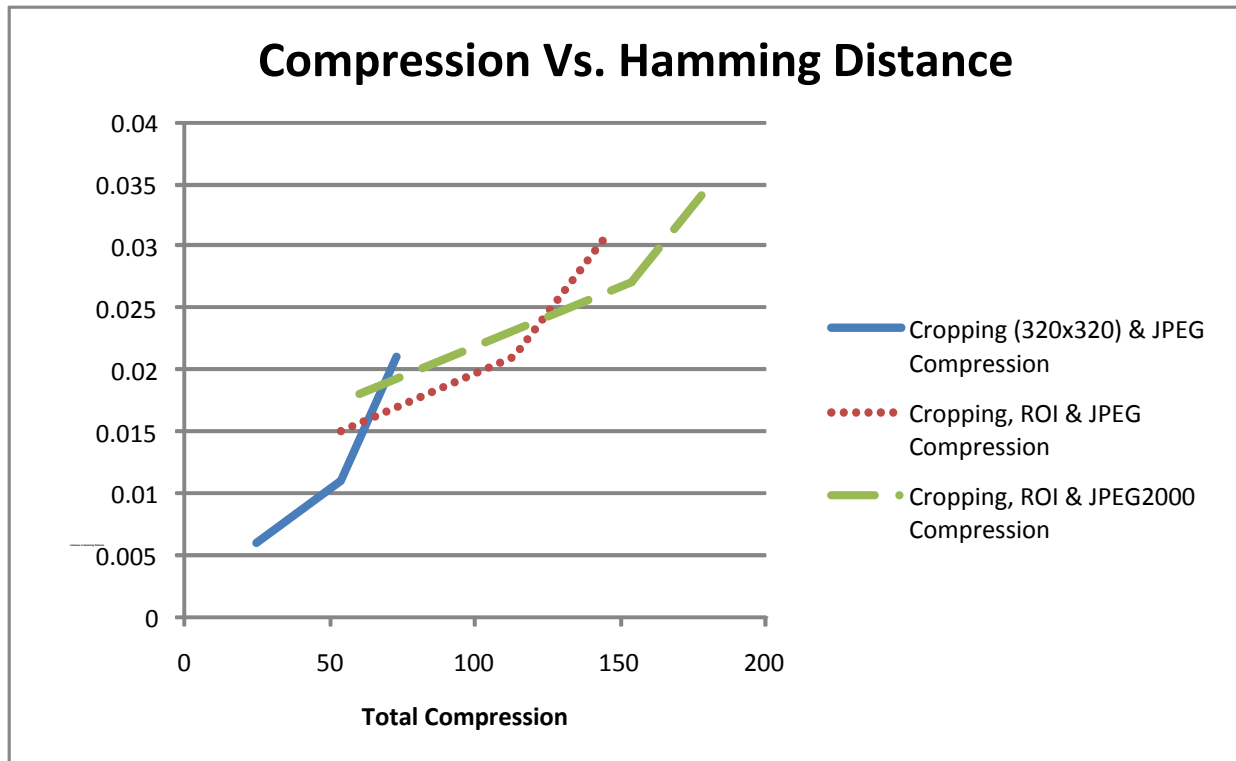
Figure 45: Hamming Distances as a Function of Compression

Strategy	Compression Parameter	Total Compression Rate	Increase In HD
Cropping (320x320) & JPEG Compression	QF = 70	24.8	0.006
	QF = 30	53.9	0.011
	QF = 20	73.1	0.021
Cropping, ROI & JPEG Compression	QF = 70	53.9	0.015
	QF = 30	113.8	0.021
	QF = 20	146.3	0.031
Cropping, ROI & JPEG2000 Compression	CF = 20	60.2	0.018
	CF = 50	153.6	0.027
	CF = 60	180.7	0.035

Figure 46: Impact of Compression of Iris Recognition Accuracy

5.4   Iris Recognition with Contact Lenses

Contact lenses with iris patterns printed on them can cause errors in the iris recognition system. Daugman has proposed a liveness test that can detects if the image has a fake iris pattern[3]. This liveness test is based on the frequency domain analysis of iris patterns. If there is a spike of high energy in some middle or high frequency range

then it means that there is a dot grid pattern caused a fake iris.

Baker *et al.* [72] have studied the effect of transparent contact lens on the recognition accuracy of several iris recognition systems. Their data was taken in the same studio with consistent ambient indoor lighting. They visually inspected all the images and reject any that were low quality. They then classified the contact-lens wearing subjects into five different categories based on a visible inspection they preformed manually.

- **Category 0** – No contact lens
- **Category 1** - minimal or no change to the iris. At most these images contain a faint visible edge.
- **Category 2** - images contain a definite circular boundary on the iris area.
- **Category 3** - contains images which the lens has writing on the lens, the lens fits improperly causing it not to lay flat on iris, or the lens produces an artifact greater than a definite ring seen in Category two.
- **Category 4** - contains the iris images where the subject is wearing hard contact lenses. Hard contacts produce a very noticeable ring and severely distort the area they cover.

They had 92 subjects that never wore contacts, 52 subjects who wore the same type of contact lenses and 32 subjects who wore contacts sometimes and didn't wear contacts for other test, and there were 3 people who changed the type of contacts they wore. In total there are 12,003 iris images from 87 contact-lens-wearing subjects and 9,697 non-contact-lens wearing subjects. 75% of the subjects were between 19 and 25 years and they have an ethnic breakdown of 36 Asian, 6 Hispanics, 122 Caucasian, and 7 subjects no reporting. There is no discussion in the paper about the time between the acquisitions of the images, however they do mention that images of hard contacts visible look different if they are acquired in different sessions.

All the images that failed to segment correctly in the IrisBEE are also removed from the dataset, but the size of the other datasets seems to suggest these images weren't all removed from the other two datasets. The data shows that a different number of images were used for each system in different test, it is unclear how or why these images are removed, particularly the 0v0 comparison of the CMU datasets. See Figure 47 for the number of images used.

| | Number of Images Used to Compare | | | | | | | | | | | |
	0v0	0v1	0v2	0v3	0v4	1v1	1v2	1v3	2v2	2v3	3v3	4v4
IrisBEE	447875	34459	15760	3000	412	311719	1114	740	211687	32	86634	42329
VeriEye	447612	34471	15801	3000	412	311908	1114	740	211747	32	86649	42442
CMU	442123	34471	15801	3000	412	311908	1114	740	211747	32	86604	42442

Figure 47: Number of iris images used to compare in each method

For analysis of these images, this test used three different recognition systems. The first was a modified version of the IrisBEE system [68, 73]. The second was the commercial VeriEye Iris SDK from Neurotechnology [60]. The third system is an iris recognition by Carnegie Mellon University[36]. The mean element is an average of the hamming distance for the IrisBEE and Carnegie Mellon system, the smaller the hamming distance the closer the images are to being a match. The mean element for the VeriEye system is match store that VeriEye provides. This score is from zero to 3235 where 3235 is an identical image and zero is not a match. In this system the average match score is about 400 and the non match score is zero. It should also be noted that in this system comparing image 1 to image 2 is not the same as comparing image 2 to image 1. So Baker et al. averaged the results of these two different permutations in every case and reported that as the results.
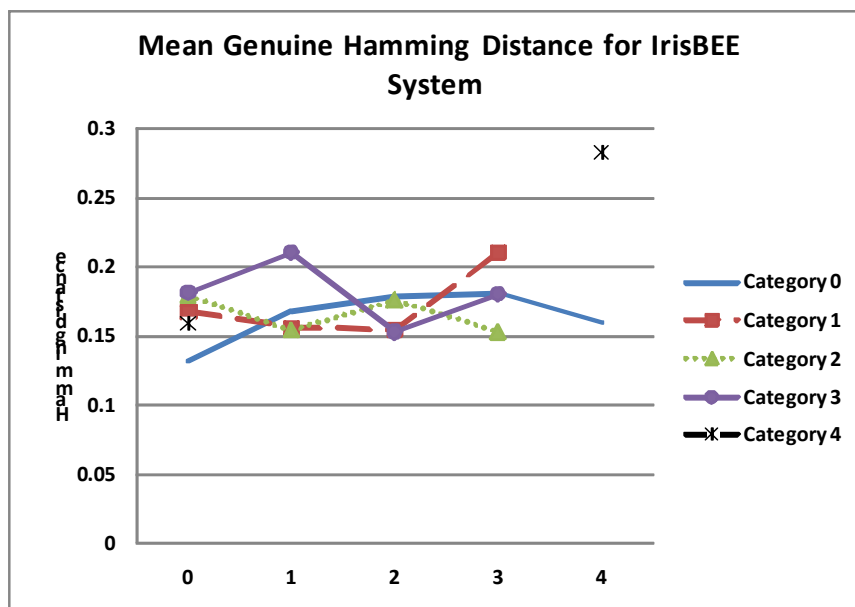
Figure 48: IrisBEE system results; Mean genuine cross matching HD, Cross matching FRR
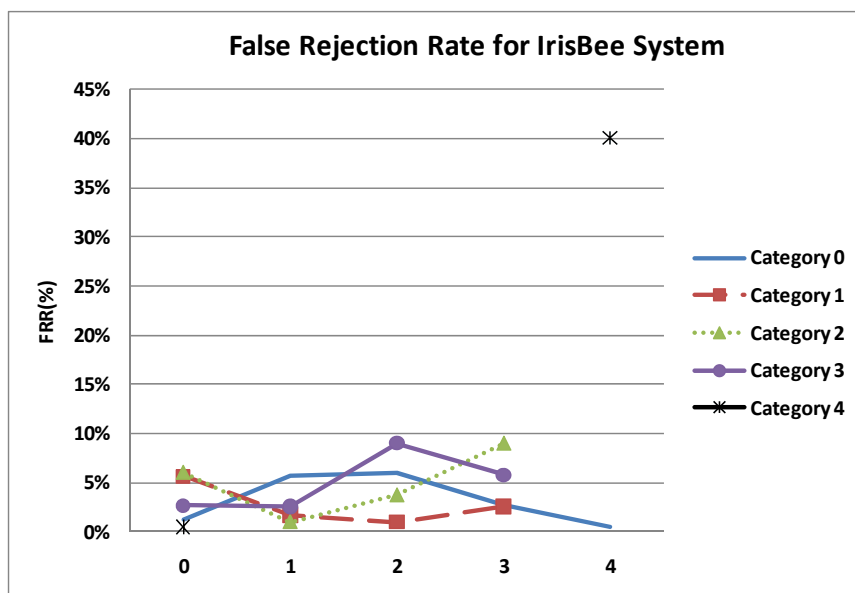

Figure 49: IrisBEE system results; Mean genuine cross matching HD, Cross matching FRR

Figure 48 shows the genuine Hamming distance, the average score for matching iris from the same iris. Each category is compared to all the other categories where data is available. Category 0 shows an increase as it is compared to worst images. This trend changes inexplicitly when it is compared to Category 4 iris. Category 1 performs similarly when compared to Category 1 or Category 2 but increases greatly when compared to Category 3. Category 2 match score improves when it matched to Category 3. Category 3 self matches performs about the same as the Category 3 to Category 0. Category 4 self matches performs the worst of any in this area.

Figure 49 the FRR for all the different cross match scores. For this test Hamming distance that is greater than 0.32 is considered to be a false rejection. In this graph the Category 0 increases when compared to Category 1 and slightly increases when compared to Category 2. Then Category 0 begins to decrease when it is compared to Category 3 and Category 4. Category 1 decreases slight when compared to Category 2 and increases when compared to Category 3. The FRR of Category 2 increase dramatically when compared to Category 3. This is unexpected because the Hamming distance for this test decreased. This must mean that there are some strong matches that help give this

group a strong Hamming distance. This might also have to do with the fact that this group has a small set of only 32. Category 3 self matches preformed worst than the category 0 or 1 but better then the category 2 match to Category 3. Category 4 has a very high FRR of over 40%.

Figure 50: VeriEye system results; Mean genuine cross matching HD, Cross matching FRR
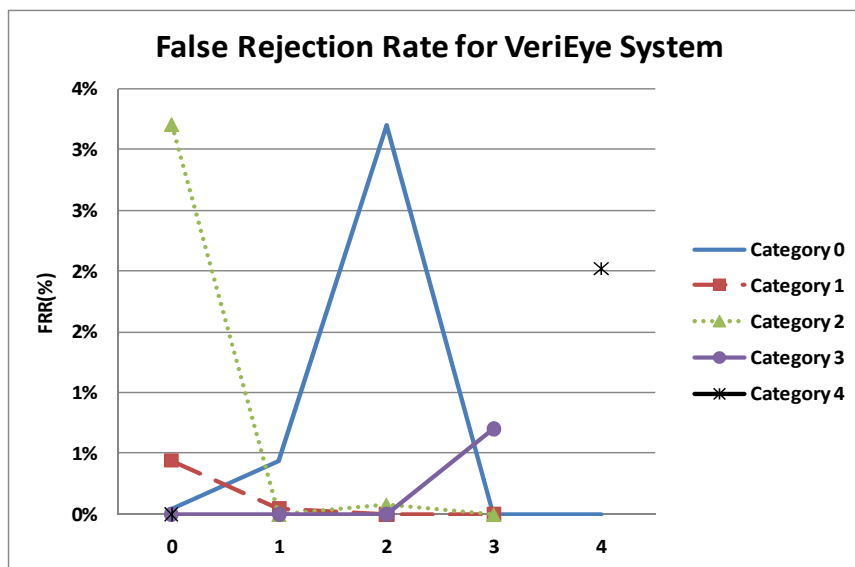
Figure 51: VeriEye system results; Mean genuine cross matching HD, Cross matching FRR

The VeriEye system performed the best on this test. Figure 50 shows the mean match score for all the tests. When comparing Category 0 to the other categories the match score decreases as the level of contact derogation increases, until category 4, when the match score improves. Category 1 decrease continuously as the level of contact derogation increases. Category 2 score decrease across the board until it is compared to Category 3, then a marked improvement is observed. The Category 4 self match performs worse than the Category 4 verse Category 1. As seen in Figure 51 the FRR of Category 0 increases until Category 3, and then it becomes zero for Category 3 and 4. Category 1's FRR also decreases to almost zero after Category 0 comparison. Category 2 follows a similar trend as Category 1. Category 3 comparison also a very low FRR until it is compared to itself, and a marked increase in FRR is observed. The FRR of Category 4 is also very high but not as bad as the Category 2 verse Category 0 comparison.
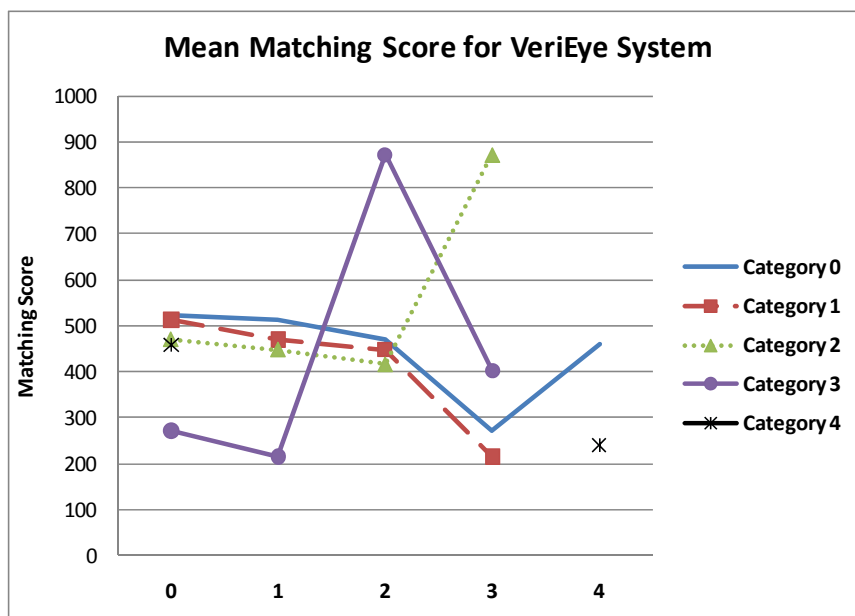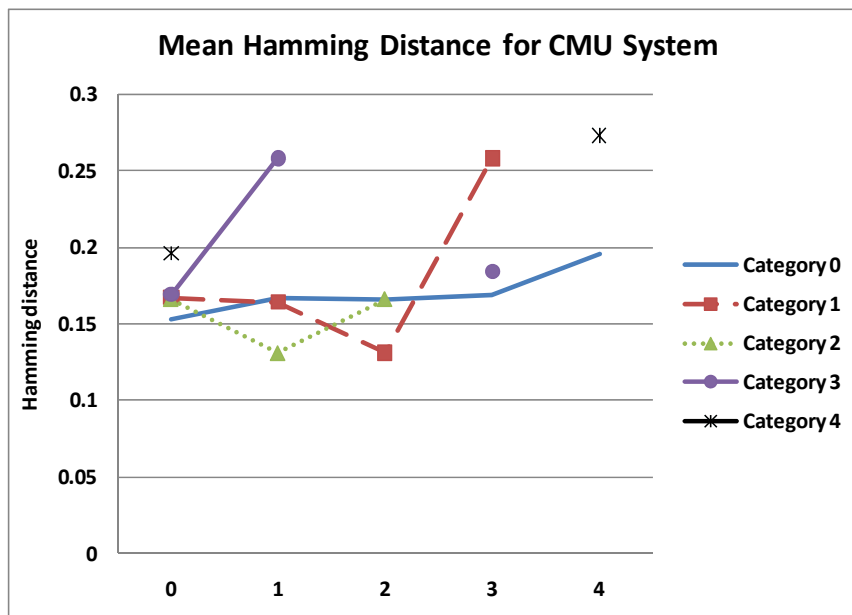
Figure 52: CMU system results; Mean genuine cross matching HD, Cross matching FRR
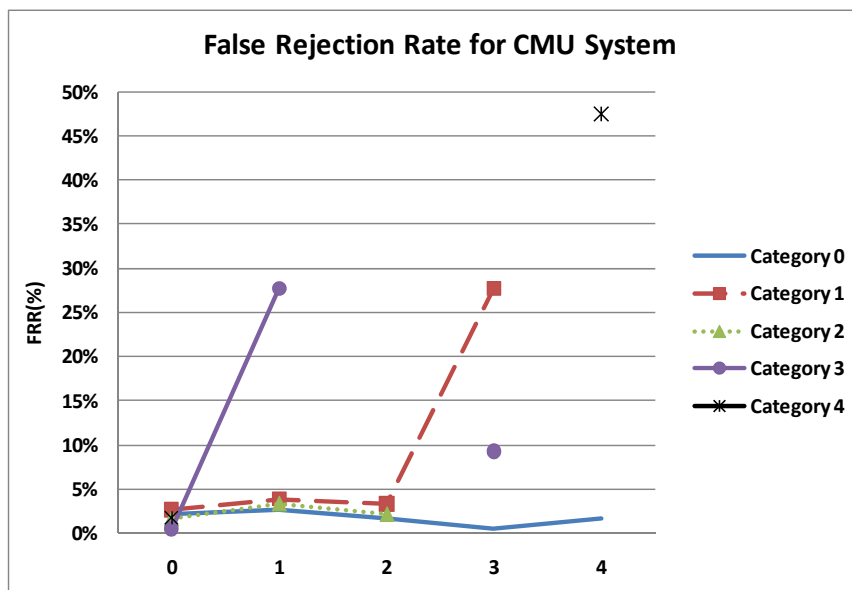
Figure 53: CMU system results; Mean genuine cross matching HD, Cross matching FRR

Finally the mean Hamming distance of the CMU system is analyzed is Figure 52. The HD of Category 0 increase as the level of contact derogation is increased. Category 1's Hamming distance improves as against Category 1 and 2, but increase as compared to Category 3. Category 2's HD decrease when compared to category 1 but increase in the self comparison. Category 3 increases from Category 0 to Category 1 comparisons. There is no Hamming distance listed for Category 2 verse Category 3 in this test only. The self comparison is slightly higher than the category 0 verse Category 3.

For FRR in the CMU see Figure 53, A false rejection for this system is a Hamming distance greater than 0.28, this is to make it comparable to the IrisBEE system. For Category 0 the FRR increased for Category 1 then decreased until Category 4, where an increase was noticed. Category 1 FRR increased slight from Category 0 to self comparison. Then the FRR decrease slight when compared to Category 2, then a large increase was observed in Category 3. Category 2 increase from Category 0 and Category 1 comparison, but decreased in the self comparison. There was a

FRR of 0% listed for the Category 2 verse Category 3, but there was no average hamming distance listed so the validity of this point is questionable. Category 4 self comparisons performed the worst.

The contact lenses introduce noise onto iris images, as the result, the ability to match the iris decreases. Their data shows that the intra-category match score always got worst as the level of the contact interference increase in all the system. The intra-category matches all have relatively large dataset this seems to be a reasonable statement.

Figure 54 has the intra-category FRR for all the systems, all the data points except for one (CMU Category 2) are increasing. They went on to say that to improve this enrolling or testing without a contact will improve this. The data shows that for Category 4 verse Category 0 always outperforms Category 4 self match dramatically and in all systems. The data set for the Category 0 verse 4 is comparatively small, only 412 images, and it is also unclear how many iris were used in this and all other tests. So they might not have enough data to say this with certainty. The other cross match scores generally don't follow this trend, they seem to increase and decrease randomly as the level of contact interference changes. This might be because the cross match scores all have smaller image sets.
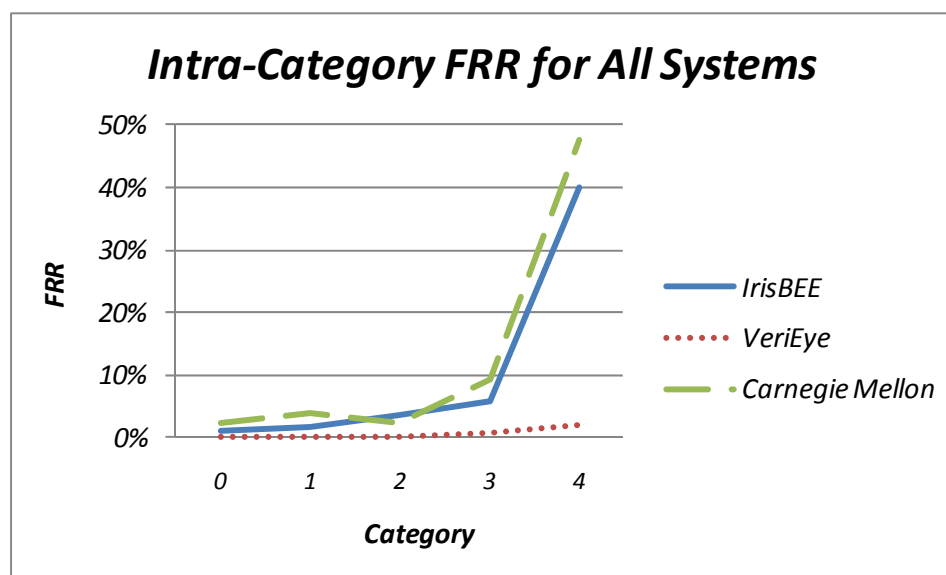
Figure 54: FRR vs. category

The false acceptance rate caused by non cosmetic prescription lenses was not discussed in depth in this paper. They show some ROC curves and false match score distribution graphs but nothing more than that. For the CMU and VeriEye system these graphs show almost no change as contacts are added, but the IrisBEE shows a definite increase in FAR when comparing Category 4 images.

5.5   Iris Recognition and Eye Disease

As a greater number of people use iris recognition systems people the likelihood of encountering people with eye disease increases. For this reason it is important to examine how eye diseases affect the recognition accuracy of iris recognition systems. Aslam et al. [74] are only researchers to study this. In this experiment pictures of diseased iris were taken and then compared to an image taken after the iris had been treated. The test consists of data from 54 individuals. To obtain the image a H100 Iris Guard portable tripod-mounted iris camera was to take a high resolution image under controlled illumination.

To compare the images Aslam used Daugmans's algorithms to process the images and find the Hamming Distance between the before and after treatment image. In this test any Hamming distance greater than 0.33 is considered to not match. There are five eyes that changed enough to make the Hamming distance greater than 0.33. In all five cases these are cases of anterior uveitis. Three of these are posterior synechiae (stuck-down iris causing pupil distortion) as shown in Figure 55. None of the other diseases caused a significant Hamming distance increase. Eyes that have had laser iridotomies and that had been pharmacologically constricted were correctly identified. Even an

eye with large inferior coloboma (developmental iris defect) was able to be identified with the Daugman algorithm. This suggests that even considerable iris abnormalities don't cause a false rejection. None of the iris with corneal disease were falsely rejected, this includes cases where corneal opacities limited the full iris feature view. The reason corneal opacities didn't affect the iris identification is that the NIR light used by the camera was less attenuated by opacities.
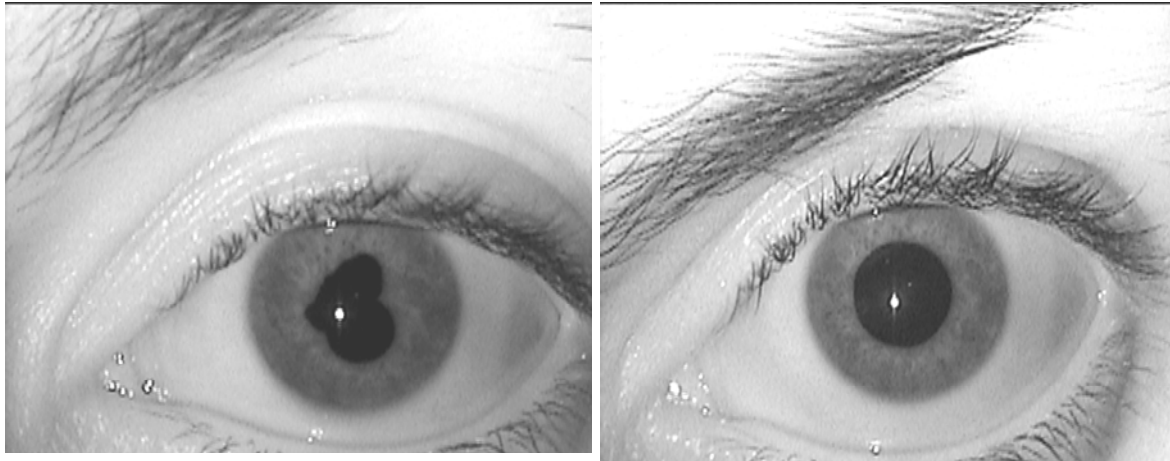
Figure 55: Example of iris pattern change before and after treatment for Synechiae [74]

Disease	# of Eyes	Mean Hamming Distance	Variance
anterior uveitis	24	0.252	0.0088
corneal disease	33	0.136	0.0030
other anterior disease	12	0.155	0.0030
control	39	0.152	0.0057

Figure 56: The average Hamming distance for each eye disease.

Figure 56 shows the hamming distance for each of the different eye diseases and the control eyes. This data clearly shows that the only significant increase in Hamming distance is caused by anterior uveitis.

5.6   Next Generation Iris Recognition Systems

5.6.1   Video-based Non-cooperative Iris Recognition

As iris recognition technologies continues to mature, it will gain the ability to acquire an image without the end user even knowing. This will make iris recognition a great way to verify people because it will cause no extra burden for the user. This technology also has great potential for finding people of interest, because a non-cooperative iris recognition system can identify people without the making the person aware they are being indentified. This application is particularly valuable for security at airport, borders or any other any public place.

Most existing iris recognition methods/systems used individual image for recognition. Some of them may use a few image frames for recognition and select the best recognition result to represent the matching result. Under non-cooperative situation, iris image quality is often low. Using single image for recognition may not achieve good recognition result.

Figure 57: The diagram of the video-based non-cooperative iris recognition system.

In [24], Du *et al.* proposed a video-based non-cooperative iris segmentation method that can quickly filter poor quality ima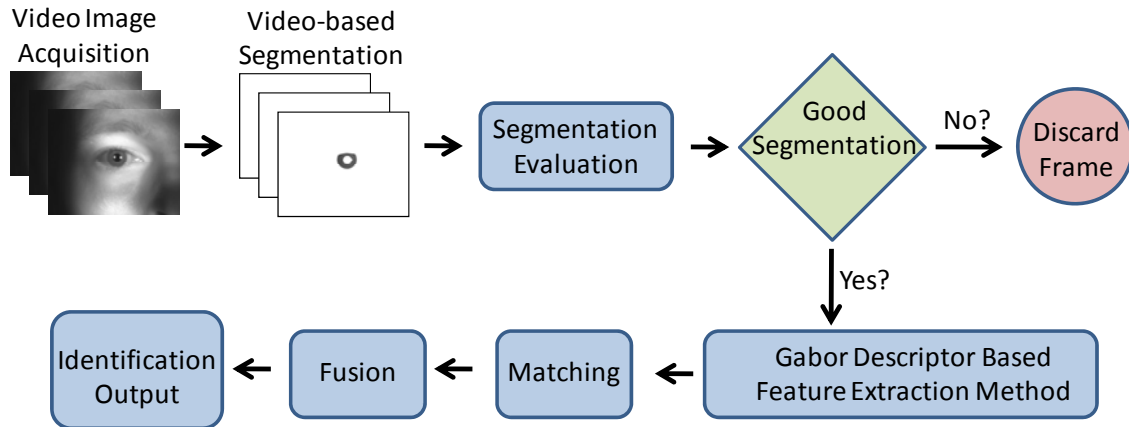ges and use coarse to fine approaches to perform accurate iris segmentation. In [40], Du *et al.* proposed using that uses video-based non-cooperative iris recognition system as shown in Figure 57. Unlike traditional approach, we used multiple enrollment images to match with input video image. The matching score between the enrollment image and the individual video frame is fused with the segmentation evaluation score. After majority vote, if the best matching score of the video to an enrollment iris satisfies the matching threshold, the matching score will be the matching result for the video to that enrollment eye. Matching results from the video sequence to other enrollment eyes will be set to 1 (1 means no-match). If even the highest matching score does not satisfy the matching threshold, this video will not be matched to any eye. The result is FAR = 0 and EER = 0 for all thresholds since only one or zero matching scores are retained for each video. 73 videos (about 24.5% of the videos) were not recognized since some videos could not generate satisfactory matching results. For the rest of the videos, there is 100% recognition accuracy (0% FAR at 0% FRR). The results show that 100% accuracy can be obtained using multiple enrollment images, video sequences of an iris, and fusion of matching scores; even in a non-cooperative iris dataset.
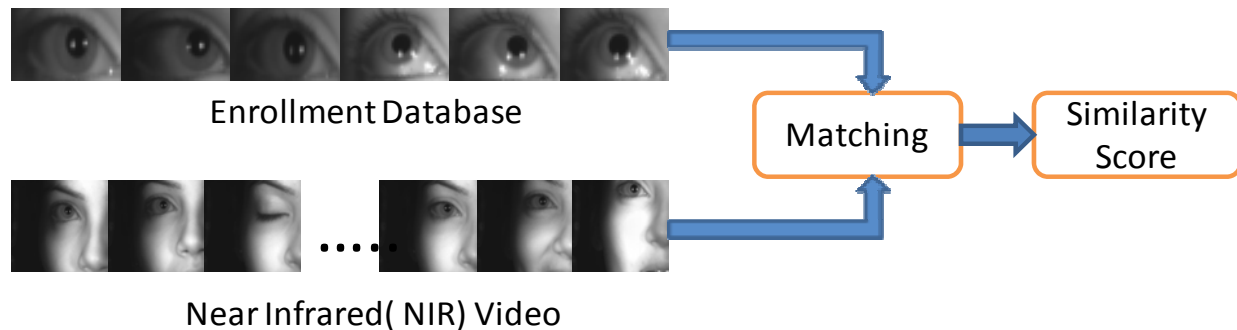

Figure 58: Matching protocol for non-cooperative iris recognition

As shown in Figure 58, future non-cooperative iris recognition systems will be able to work from a greater distance. As this technology continues to improve it even has the potential to scan large groups of people for target individuals.

5.6.2   Multiple Wavelength Based Iris Recognition

NIR images have been dominant in iris identification [75]. One downside to NIR light is it requires active NIR illumination. Visible wavelength iris recognition could function using environmental illumination. In addition, visible wavelength recognition is important because it can be used with facial recognition for multimodal biometrics. In the future regular color surveillance camera may have the capability to perform iris recognition.

Visible wavelength iris recognition has its own challenges, especially it is challenging for dark color eyes and remote iris recognition. Proenca has discussed several issues using visible wavelength in [75]. He performed iris segmentation in unconstrained situation acquired at-a-distance and on-the-move. Rather than segmenting the pupil first, like many NIR systems do Proenca first detected the sclera. The information about the sclera was then used to find the iris. The data is processed with a multilayered feed-forward neural network to calculate the location of the sclera. Proenca then calculated how many sclera pixels are left, right, above and below each non-sclera pixel. By looking at the regions that have a significant amount sclera to the left and right it is possible to find the iris region. A polynomial regression on the polar coordinate system was then run in order to segment the shape of the iris. To find the center of the iris was found by summing the binary image of the iris in the x and y directions and calculating the maximum. From there the image is put into polar coordinates and a polynomial is fit to the data points. However in [12], Procenca and Alexandre showed that the iris recognition in visible wavelengths are still very challenging and the accuracy is much lower than recognition result in NIR wavelengths, especially for dark color eyes.

Chou *et al.* proposed to use RGB and NIR images together for iris recognition [9]. In this paper a four-spectral camera was used to capture non orthogonal view images. The first step in their process was segmenting the pupil. A binary threshold was then performed on the NIR image. Morphology is then performed on the binary image to find areas that are the size and in the right location. Finally an ellipse fitting algorithm was used to find the boundary of the final pupil candidate. An affine transformation is the next step of their process. This process turns the elliptical pupil into a circle. This is done my first rotating the image so the major axis of the ellipse is vertical and the minor axis is horizontal. Then the image is stretched horizontally so the minor axis is as long as the major axis. Then the image is rotated back to its original orientation. Chou *et al.* designed the Intelligent Random Sample Consensus or RANSAC for limbic boundary recognition. This method uses the four-spectral measurements rather than the orientation of the edge filter, like tradition intelligent iris segmentation systems. Like most iris recognition rubber sheet method is used to normalize the mask and the image in polar coordinates. For encoding the image edge-type descriptor are used. Because of noise that could be in the image only the vertical edges are used in their test. The two filters they used are derivative of Gaussian and Laplacian of Gaussian. The filters are then convolved with the images to get filtered images. If the filtered images have intensity greater than 0 it is likely that there is a ridge at that location. For matching the Daugman hamming distance is used.

In the future, multiple-wavelength iris recognition may attack more attention and can work with multiple-wavelength face recognition together for video surveillance.

5.6.3   Multimodal Eye Recognition

Multimodal biometrics is introduced in 1998 to combine multiple biometrics to do positive human identification in commercial applications. By using more than one means of biometric identification, the multimodal biometric identifier can obtain high recognition accuracy. However, choosing reliable biometric identifiers is still a question in multimodal biometrics.

Since the iris patterns of dark color eyes could reveal rich and complex patterns only under NIR light, if the NIR iris image be obtained in long distance, the accuracy of iris recognition will drop dramatically. And if we acquire iris image in visible light, the iris patterns of dark color eyes will be hardly visible under visual light.

In [76], Thomas *et al.* showed that the sclera, the white and opaque outer protective covering of the eye, can also be used in human identification. They designed an illumination-, orientation–, translation–, and deformation–invariant sclera recognition method. In [77], Zhou et al. proposed a multimodal eye recognition method by fusing sclera and iris recognition. Figure 59 shows the process of multimodal eye recognition system.
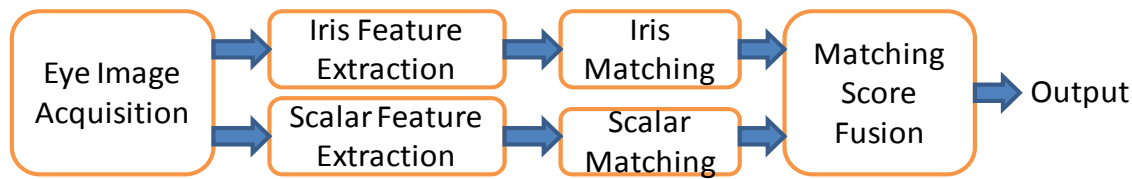
Figure 59: Multimodal eye recognition system..

For iris recognition, a typical iris recognition method can be used. The diagram of the sclera recognition system is shown in Figure 60, which includes segmentation, feature extraction, and feature matching.
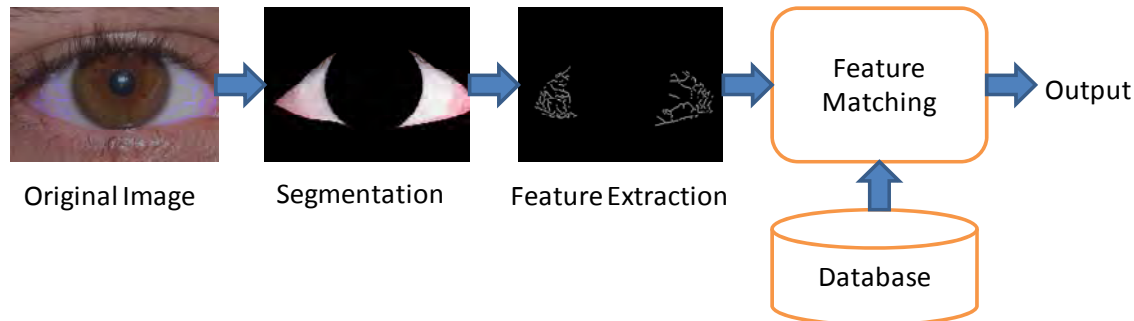

Figure 60: The sclera recognition system

For the sclera image segmentation process, it includes image downsampling, conversion to the HSV color space, estimation of the sclera region, iris and eyelid detection, eyelid and iris boundary refinement, mask creation, and mask upsampling. The sclera region is estimated using the best representation between two color-based techniques.

For the sclera vein pattern enhancement, a bank of multiple directional Gabor filters is used for vascular pattern enhancement. For the sclera feature extraction, a line descriptor approach is proposed. The line segments are described by three quantities – the line segments' angle to some reference angle at the pupil center, the line segments' distance to the pupil center, and the dominant angular orientation of the line segment. The total descriptor for the sclera vein structure is the set of all of the individual segments' descriptors.

For sclera template matching, a new method based on a RANSAC-type algorithm is developed to estimate the best-fit parameters for registration between the two sclera vascular patterns.

In multimodal biometrics score fusion part, since matching scores of iris recognition and sclera recognition are not in the same range, Min-Max (MM) method is applied to do score normalization. After that, Kernel-based matching score fusion of iris matching score and sclera matching score is used to improve the performance of eye recognition system. The experimental results show that the proposed eye recognition method can achieve better performance compared to unimodal biometric, and the accuracy of proposed kernel-based matching score fusion method is higher than other traditional methods.

Other methods of multimodal biometrics are also used, such as fingerprint/iris, and fingerprint/iris/face. In the future, more kinds of multimodal biometric systems will be designed/developed to achieve high recognition accuracy, be more user friendly, and provide more flexibility in applications.

5.7   Conclusions and Acknowledgements

In this section we preformed thorough literary review of iris segmentation, feature extraction, template generation, matching and quality measures. Then the study of the state-of-the-art system was conducted, which includes a test and analysis of a commercial system using seven datasets and a summary of available commercial systems. Some of the challenges of existing systems were also covered in this section. Finally, new trends in iris recognition were discussed.

We investigated the vulnerabilities of state-of-the-art iris recognition system over compression, contact lenses and eye diseases. Then we discussed non-cooperative iris recognition, iris recognition in the visible light spectra, multiple wavelength iris recognition and multimodal biometric approaches.

In conclusion, iris recognition has proven to be an accurate and reliable biometric method. Our extensive study of iris recognition systems has proven current systems are able to accurately recognize people in well controlled situations. Advances in iris recognition technology will allow even higher accuracy and more ruggedized system. By utilizing different spectra of light and multimodal biometrics there will be a great number of applications for biometrics. Non-cooperative iris recognition is an emerging area that can make iris recognition more user friendly and flexible, and make it even possible for iris-based video surveillance.

The research in section uses the ICE 2005 [68] and MBGC 2008 [66] datasets provided by NIST, CASIA 2.0 and CASIA 3.0 iris image dataset collected by the Institute of Automation, Chinese Academy of Sciences [69], WVU dataset provided by Dr. A. Ross at West Virginia University [65], and UBIRIS dataset provided by the Department of Computer Science at the University of Beira Interior [39]. We will also like to thank the people who contributed their sclera data for and IUPUI Multi-wavelength and IUPUI remote dataset.

6 GenKey Fingerprint-Based PET Performance Evaluation

6.1 GenKey Technology

GenKey, a leading provider of biometric PET solution, was founded in 2001 as a division of the Norwegian Software as a Service (SaaS) company Meltwater. The company has developed a biocryptic algorithm that bridges cryptology with biometrics. This patented algorithm converts a biometric image into Public Key Infrastructure (PKI)-compatible crypto keys that are irreversible and share no mathematical relationship with the biometric sources they represent. Its solutions, branded as Biocryptic ID Management Systems (BIDS), can be applied to a variety of contexts including education, licensing and healthcare.

The GenKey algorithm provides a means to enroll and verify individuals based on biometric information, such as a fingerprint. The algorithm offers a number of options which provide tradeoffs between recognition speed, accuracy, and biometric privacy.

6.1.1 GenKey Feature Template vs. ID Key Enrollments

The GenKey algorithm can perform two types of enrollment. In feature template enrollment, discriminating features from fingerprint images are extracted and stored as the individual's biometric template. The feature template is stored for later use and the biometric image may be discarded.

ID Key enrollment also extracts discriminating features from fingerprint images, but converts features into a numerical value which represents the individual's biometric. At the conclusion of an ID Key enrollment, the ID Key (numerical value) is stored and the biometric image and feature template may be discarded. This type of enrollment is focus of IBG's performance evaluation.

During ID Key enrollment, an enrollee in provides one or more images from one or more fingers. These sample fingerprint images are first converted to feature templates as described earlier. The enrollment feature templates from all fingers to be enrolled are then combined into a single digit or key that represents the set of provided enrollment fingers. This ID Key can then be stored for later use during verification or identification, as show in Figure 61.
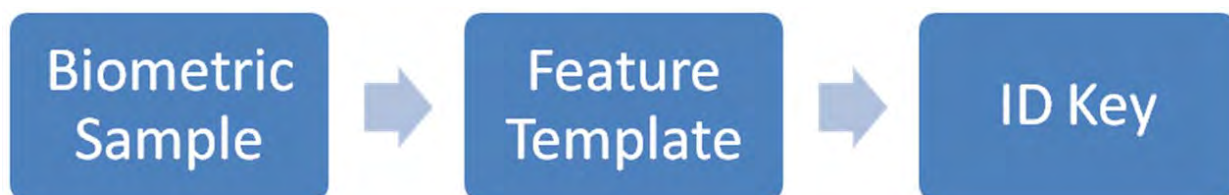
Figure 61: ID Key Generation Process

An ID Key created from multiple fingerprint positions is referred to as a fusion key. Multiple fingerprint positions generally provide higher verification accuracy than a single fingerprint position.

During verification, the individual provides one or more enrolled fingerprints. The GenKey algorithm analyzes the images and creates a feature template. The feature template and ID Key are provided to the GenKey algorithm and a binary verification decision is returned.

For ID Keys, balancing the tradeoff between FAR and FRR is accomplished through an FAR control parameter provided to the algorithm. Keys are created with respect to a particular FAR control parameter. The value of the FAR control parameter ranges from 0.0 to 1.0; lower values correspond to lower FAR (and higher FRR). The FAR control parameter is only applicable at enrollment. As a result, adjusting the FAR threshold will not impact the error characteristics of keys that have already been enrolled.

In keeping with the Study's focus on the commercial viability of PETs for defence applications, IBG tested two GenKey ID Key types:

- **Standard ID Key**s offer performance near the performance of the feature template enrollments.
- **Flex ID Key**s tradeoff key size and accuracy.

Various Flex ID Key sizes can be configured to meet the storage needs of the application, and the GenKey library will maximize accuracy for the given key size automatically. Flex ID Keys provide similar accuracy performance as Standard ID Keys but in a slightly smaller footprint. Flex ID keys are designed to maintain reasonable performance levels even at substantially reduced key sizes. From a product development perspective, with the introduction of Flex ID Key, GenKey notes the Standard ID Key will be phased out in future releases. The two types of ID Keys, along with GenKey's traditional feature-based enrollment, are compared in Figure 62.

	Feature Template (not a PET)	Standard ID Key (PET)	Flex ID Key (PET)
Accuracy	Feature enrollments provide the most robust performance.	Standard ID Keys will perform at only slightly degraded error rates as compared to feature templates.	Flex ID Keys provide a range of accuracy performance options. The largest Flex ID Keys provide accuracy similar to Standard ID Keys.
Privacy	Offers some privacy protection for the fingerprint; having access to a feature template does not provide a malicious user with capability to reconstruct the original fingerprint. With detailed knowledge of the GenKey feature template creation process, a malicious user could gain access to general information about the fingerprint structure.	ID Keys offer a privacy advantage over feature template enrollment. A malicious user with access to the ID Key cannot practically regenerate the fingerprint features or extract any detailed information about the fingerprint structure. The technique used to convert the feature template to a key is analogous to a cryptographic one-way function. It is easy to compute an ID Key from a feature template; however, reversing this process is computationally infeasible.	
Throughput	Feature enrollments offer the fastest search speeds. The GenKey algorithm is capable of performing millions of feature template matches per second using ordinary computer hardware.	While not as fast as feature template matching, ID Key verifications can also be performed at relatively high speeds using ordinary computer hardware; GenKey estimates rates of hundreds of thousands of verifications per second. Match speed increases (i.e. becomes slower) as stricter match thresholds are applied.	
Typical Key Size	128-256 bytes	64-128 bytes	12-107 bytes

Figure 62: Standard and Flex ID Tradeoff

The performance of the GenKey algorithm was evaluated using the following ID Key configurations:

- Standard ID
- Flex ID 12 bytes
- Flex ID 25 bytes
- Flex ID 56 bytes
- Flex ID 107 bytes

6.2 Methodology

6.2.1 Test Data

IBG has a collection of approximately 20,000 flat fingerprint images (left and right index, middle, and thumb) from 1,200 subjects collected under indoor office conditions. Fingerprint images were collected through a 500dpi Cross Match Verifier. Each subject provided two samples per position during a first visit. Additionally, approximately 650 of the 1,200 subjects provided two samples per position during a second visit which occurred roughly one month after the first.

Images were inspected at the time of capture for quality, but no automated quality checks were implemented. Therefore data quality is variable.

In addition to processing through the GenKey algorithm, IBG processed the same fingerprint dataset through a widely-adopted, minutiae-based fingerprint algorithm –Neuortechnology VeriFinger version 6.3. The VeriFinger processing approach was equivalent to the GenKey approach described below. Comparing and contrasting GenKey results with VeriFinger results will provide a general frame of reference for validating the commercial viability of GenKey's ID Key technology.

6.2.2 Enrollment Process

Using a Software Development Kit (SDK) provided by GenKey, IBG developed a custom application that performed feature extraction, template creation, and ID Key creation. First-visit fingerprint images were used for enrollment and ID Key creation. As shown in Figure 63, two different images for each position were used to create a generalized enrollment. This increases matching accuracy and is consistent with GenKey usage in operational deployments.
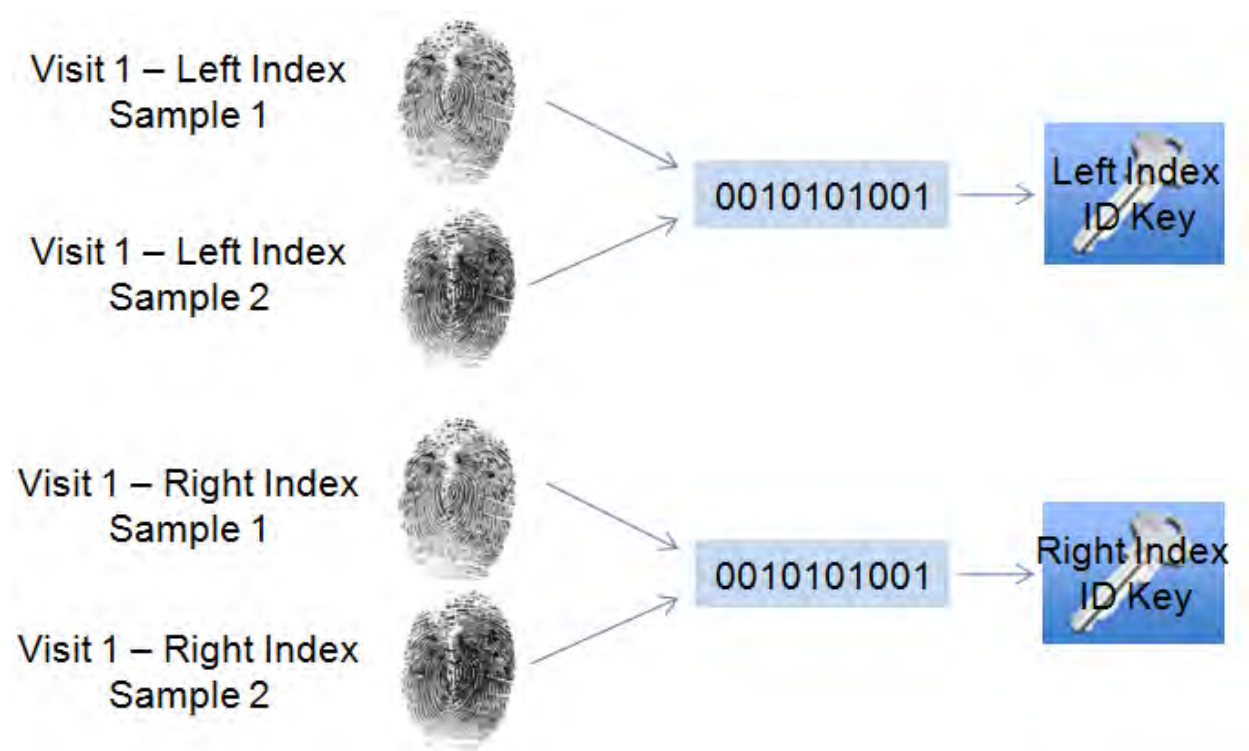
Figure 63: Enrollment Transaction Logic

Both index fingerprints had to enroll in order for an enrollment to be successful.

6.2.3 Recognition Process

IBG developed a custom application that performed bulk matching. Second-visit fingerprint images were used for recognition (i.e. as probe images) are compared against first-visit fingerprint data.
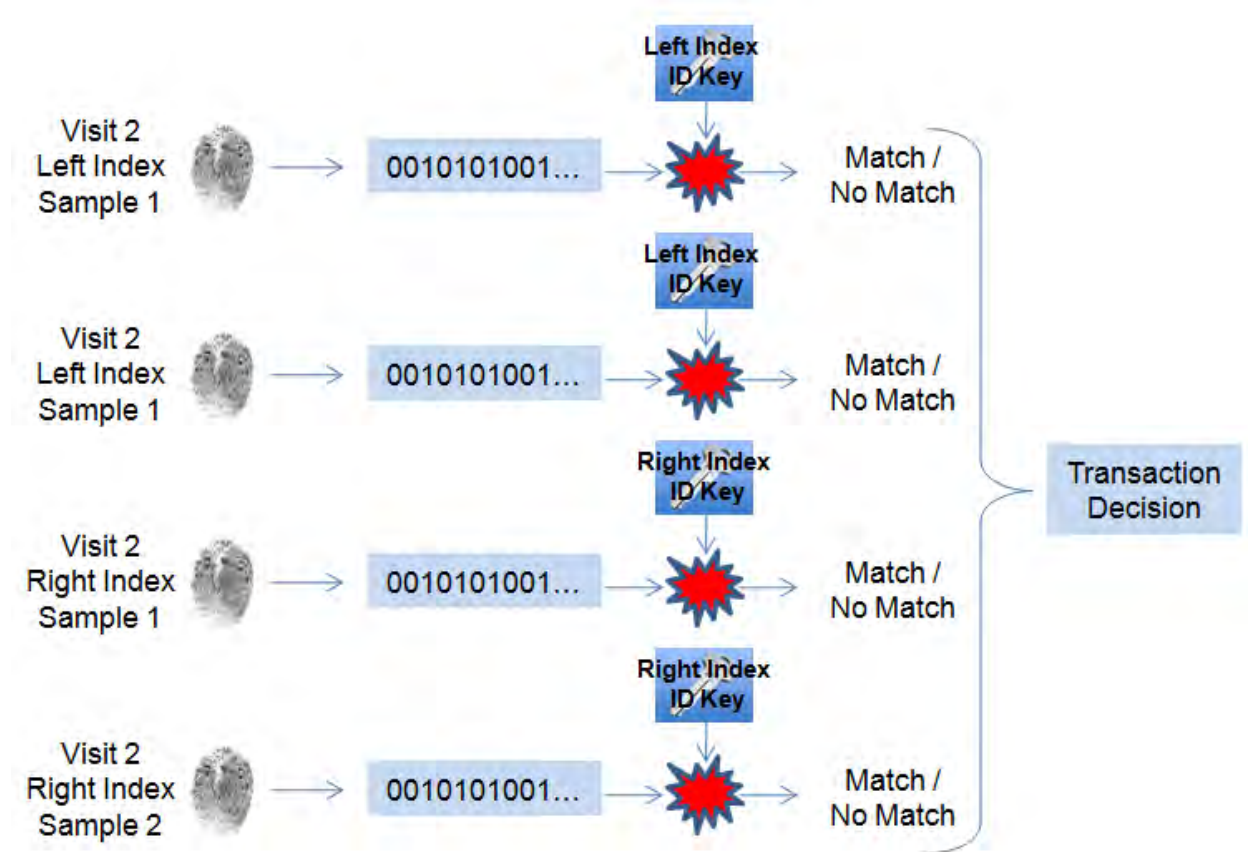
Figure 64: Recognition Transaction Logic

As shown in Figure 64, verification was based on the following two-position logic:

$$\text{Verification}(g_r, g_l, a_r, a_l) = \begin{cases} \text{True} & \text{if } g_r \boxdot a_r \text{ OR } g_l \boxdot a_l \\ \text{False} & \text{if } g_r \boxdot a_r \text{ AND } g_l \boxdot a_l \end{cases}$$

Where a match is denoted by $\boxdot$ and a non-match is denoted by $\boxdot$.

$g_r =$ Right Index Gallery Template
$g_l =$ Left Index Gallery Template
$a_r =$ [Right Index Attempt 1, Right Index Attempt 2]
$a_l =$ [Left Index Attempt 1, Left Index Attempt 2]

If any match occurred between a sample and an ID Key, the transaction was declared a match. If all samples failed to match their respective ID Keys, the transaction was declared a non-match. All comparisons were intra-position, meaning that (for example) index fingerprints were never compared against middle fingers.

Processing volumes (less quality failures and missing positions) as shown in Figure 65.

	GenKey	VeriFinger 6.N

Subjects	650	650
V1 Samples	2	2
V2 Samples	2	2
Positions	2	2
Genuine comparisons	456	459
Impostor Comparisons	550976	560741

Figure 65: Fingerprint Test Parameters

Metrics

Based on collection and comparison processes described above, metrics were generated as shown in Figure 66

Usability Metrics	Accuracy Metrics
• Failure to Encode Rate (FTE) • Failure to Acquire Rate (FTA) • Processing Time	• False Match Rate (FMR) • False Non-Match Rate (FNMR) • Matching Error Rates by Position • Distribution of Errors by Subject

Figure 66: Fingerprint Test Metrics

6.3   Results

6.3.1   Throughput

The most relevant timing metric for GenKey is time to generate a feature template (i.e. encoding or enrollment time). At operationally relevant security levels, GenKey averaged approximately 400ms per image. In a 1:1 system, this process time can be considered trivial.

6.3.2   Enrollment and Encoding Rates

This section presents results for enrollment and encoding rates. These rates can be discussed at the image level and at the transaction level.

At the image level:

- Failure-To-Enroll Rate (FTE) is the proportion of enrollment transactions in which the test subject failed to enroll
- Failure-To-Acquire Rate (FTA) is the proportion of recognition transactions in which the test subject failure to encode

At the transaction level:

- A transactional failure to enroll occurred if zero fingerprint positions were able to generate a template or key during enrollment
- A transactional failure to acquire occurred if either fingerprint position failed recognition-phase encoding (in a live-capture system, this is referred to as acquisition)

Image-level FTE rates are shown in Figure 67.

	Enrollment Attempts	FTE Count	FTE Rate
VeriFinger 6.3	2448	42	1.72%
GenKey ID Key	2448	45	1.84%

Figure 67: Comparative Fingerprint FTE

Image-level FTA rates are shown n Figure 68.

	Recognition Encoding Attempts	FTA Count	FTA Rate
VeriFinger 6.3	1841	1	0.05%
GenKey ID Key	1841	66	3.59%

Figure 68: Comparative Fingerprint FTA

Results show that GenKey and Verifinger FTE are roughly equivalent, while GenKey FTA is substantially higher than VeriFinger FTA. This underscores the concept that GenKey is predicated on the use of high-quality images whose quality is validated in real time at the point of capture.

6.3.3 Quality of Enrolled Images

Figure 69 shows GenKey-generated quality values for encoded images. Quality values range from 0-1 and are binned by 0.1 for clarity. Results suggest that as long as images are of sufficient quality to create a reference template, that GenKey will bin the image as high-quality.

Figure 69: Quality of Encoded Fingerprint Images

Figure 69 shows GenKey-generated quality values for encoded images. Quality values range from 0-1 and are binned by 0.1 for clarity. Results suggest that as long as images are of sufficient quality to create a reference template, that GenKey will bin the image as high-quality.
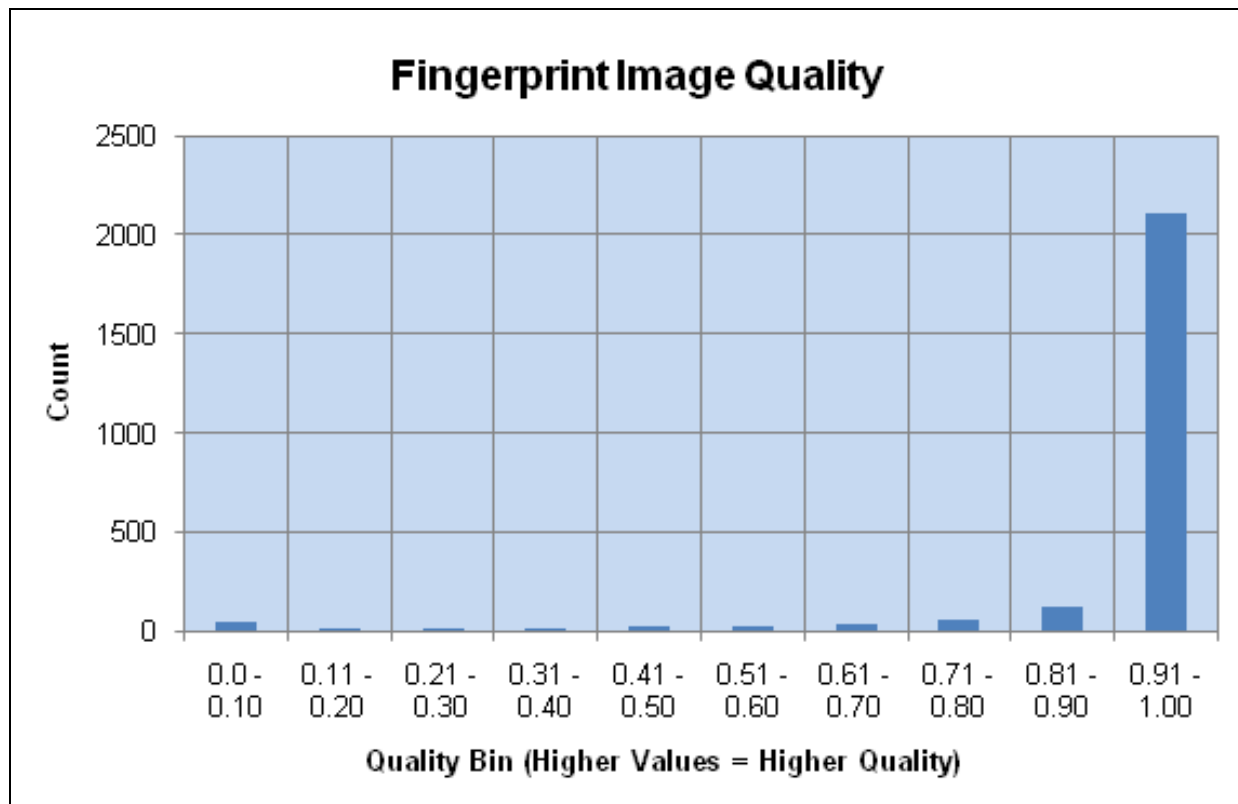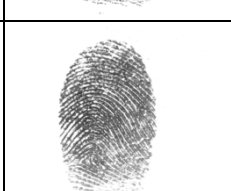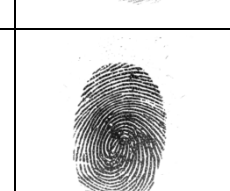
Quality Level					
0.0-0.2					
0.2-0.4					
0.4-0.6					
0.6-0.8					
0.8-1.0					

Figure 70: Examples of Image Quality from 0.0 to 1.0

6.3.4 Accuracy Rates

Figure 71 presents FNMR at specific FMR values. Systems are frequently evaluated based on their genuine error rates at specific impostor error rates. Many systems are configured to provide 0.10% or 0.01% FMR, such that the likelihood of a false match is 1 in 1000 or 1 in 10,000 (respectively). Therefore it is useful to examine genuine error rates at these specific impostor error rates. Error rates presented in this section do not include acquisition failures (FTA or FTE).

	Genuine Error Rates at 0.10% FMR	Genuine Error Rates at 0.01% FMR
VeriFinger 6.N	1.74%	1.74%
GenKey Standard ID Key	2.19%	2.85%
GenKey Flex ID Key 107 Byte	1.54%	2.41%
GenKey Flex ID Key 56 Byte	1.75%	2.63%
GenKey Flex ID Key 25 Byte	2.85%	6.80%
GenKey Flex ID Key 12 Byte	7.89%	20.18%

Figure 71: FNMR at Vendor-Specified FMR Thresholds

Figure 72 shows GenKey results at each evaluated threshold. Values in bold, in the range of Threshold values from 0.30 to 0.50, can be considered operationally relevant.

	Standard		Flex-ID 107 byte		Flex-ID 56 byte		Flex-ID 25 byte		Flex-ID 12 byte	
Threshold	**T-FMR**	**T-FNMR**	**T-FMR**	**T-FNMR**	**T-FMR**	**T-FNMR**	**T-FMR**	**T-FNMR**	**T-FMR**	**T-FNMR**
0.00	0.00%	43.86%	0.00%	39.47%	0.00%	40.35%	0.00%	50.88%	0.00%	64.25%
0.05	0.00%	33.77%	0.00%	32.24%	0.00%	32.89%	0.00%	42.54%	0.00%	55.92%
0.10	0.00%	27.19%	0.00%	23.68%	0.00%	24.34%	0.00%	33.77%	0.00%	47.59%
0.15	0.00%	20.83%	0.00%	17.98%	0.00%	18.42%	0.00%	23.90%	0.00%	39.25%
0.20	0.00%	13.60%	0.00%	10.75%	0.00%	11.40%	0.00%	16.01%	0.00%	28.29%
0.25	0.00%	8.99%	0.00%	6.80%	0.00%	7.24%	0.00%	9.87%	0.01%	20.18%
0.30	**0.00%**	**5.04%**	**0.00%**	**3.51%**	**0.00%**	**3.95%**	**0.01%**	**6.80%**	**0.02%**	**13.60%**
0.35	**0.02%**	**2.85%**	**0.03%**	**2.41%**	**0.03%**	**2.63%**	**0.03%**	**4.39%**	**0.07%**	**7.89%**
0.40	**0.09%**	**2.19%**	**0.14%**	**1.54%**	**0.14%**	**1.75%**	**0.12%**	**2.85%**	**0.23%**	**4.39%**
0.45	**0.38%**	**0.88%**	**0.56%**	**0.88%**	**0.56%**	**1.10%**	**0.44%**	**1.54%**	**0.74%**	**2.63%**
0.50	**1.91%**	**0.44%**	**2.51%**	**0.22%**	**2.49%**	**0.44%**	**1.72%**	**0.88%**	**2.85%**	**1.32%**
0.55	3.21%	0.22%	4.07%	0.22%	4.04%	0.22%	2.71%	0.66%	4.34%	1.10%
0.60	5.26%	0.00%	6.51%	0.00%	6.46%	0.00%	4.29%	0.44%	6.39%	1.10%
0.65	8.22%	0.00%	9.88%	0.00%	9.81%	0.00%	6.68%	0.22%	9.01%	1.10%
0.70	12.30%	0.00%	14.44%	0.00%	14.34%	0.00%	9.78%	0.00%	11.93%	1.10%
0.75	19.13%	0.00%	21.83%	0.00%	21.70%	0.00%	14.71%	0.00%	15.56%	0.44%
0.80	27.22%	0.00%	30.56%	0.00%	30.40%	0.00%	21.20%	0.00%	18.92%	0.44%
0.85	42.65%	0.00%	45.99%	0.00%	45.79%	0.00%	34.55%	0.00%	23.52%	0.22%
0.90	54.70%	0.00%	56.71%	0.00%	56.51%	0.00%	45.80%	0.00%	26.78%	0.22%
0.95	63.38%	0.00%	63.71%	0.00%	63.48%	0.00%	55.39%	0.00%	30.11%	0.22%
1.90	70.76%	0.00%	70.69%	0.00%	70.46%	0.00%	62.51%	0.00%	42.81%	0.22%

Figure 72: GenKey Matching Accuracy (Table)

Performance in the following section is rendered through results tables and detection error tradeoff (DET) curves. The range of thresholds was selected based on the incidence of observed errors and on consideration of operationally realistic values. DET curves plot error pairs (e.g. FNMR and FMR) across a range of values. Left- and lower-most DET curves indicate lower comparison error rates. DET curves can be used to identify the point at which one wishes to operate one's system – e.g. at 0.01% FMR or 1.00% FNMR – and estimate the corresponding genuine or impostor error rate at that operating point.

While DET curves will ideally be smooth through the full range of performance, at the right- and bottom-hand side of the curve, plots may become "stepped", indicating that the number of genuine or impostor errors at these points is unchanged while the counterpart error type changes. In order to maintain readability and to focus on reasonable or differentiated performance ranges, the DETs below show error rates across the following ranges:

- T-FNMR: 0.1% to 10%
- T-FMR: 0.01% to 10%

False non-match rates and false match rates are calculated by dividing the number of errors at a given threshold by the total number of genuine and impostor comparisons executed, respectively. The total number of genuine and impostor comparisons executed for each comparison type precedes each results table. In many operational deployments, users are permitted to execute multiple attempts, such that FNMR is lower than observed in single-attempt tests. If the Report reader were to focus on either attempt-level or transactional comparison error rates, the latter is more operationally realistic.

Figure 73 shows the same GenKey matching results in chart form, and also adds results for Neurotechnology VeriFinger.
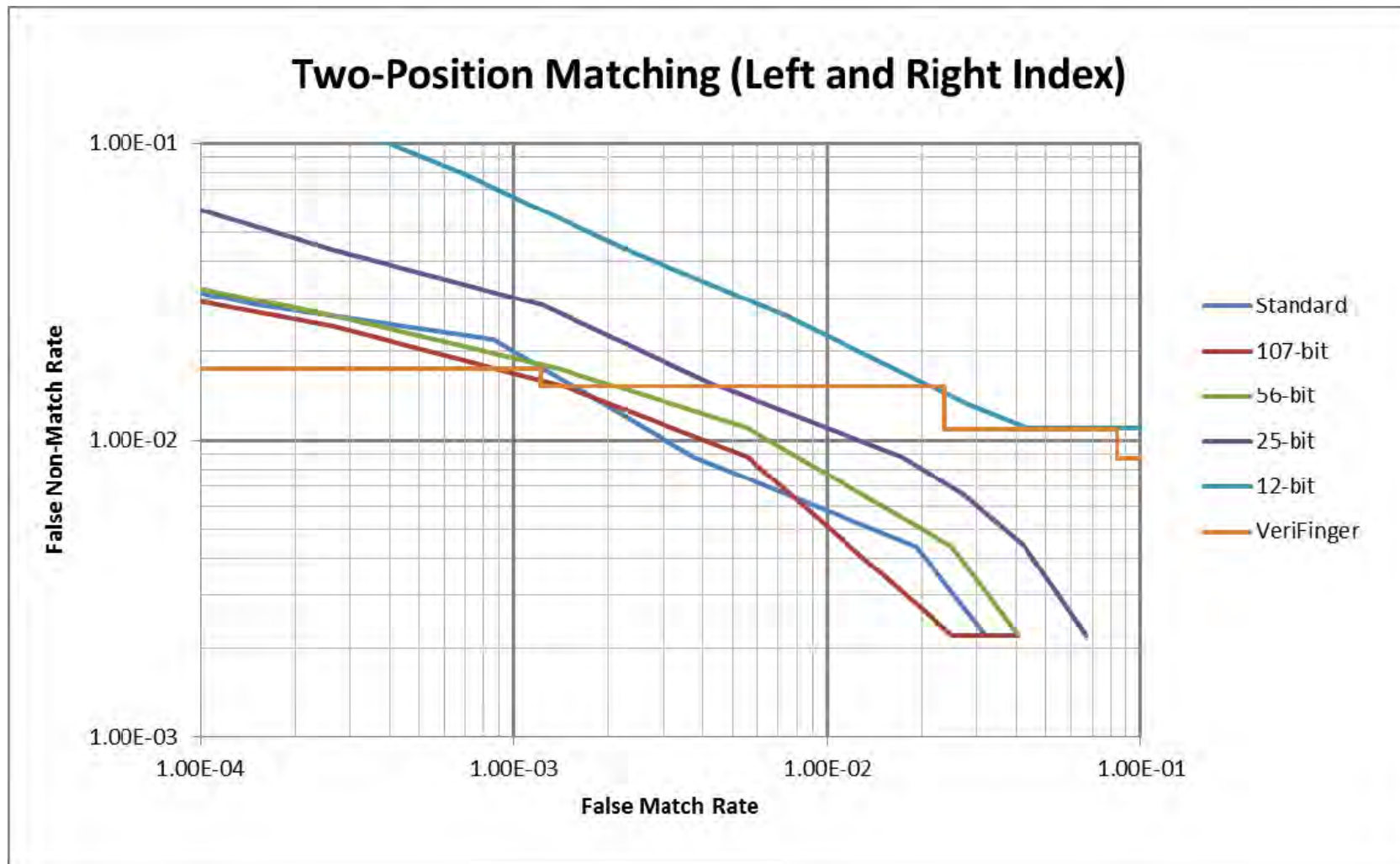
Figure 73: GenKey Matching Accuracy (DET)

6.3.5   False Match Rates by Subject

For many biometric systems, certain subjects encounter higher false match rates than others. IBG analyzed the distribution of false matches across subjects. Subject-specific false match rates (aggregated across all evaluated ID Key types and sizes, and measured at a typical threshold of 0.45) ranged from as high as 4.04% and as low as 0.00%. The ten Test Subjects with the highest false match rates are shown in Figure 74. While false match rates generally decline as key sizes increase, in some cases subjects encountered higher false match rates at larger key sizes. For example, 251 of 457 subjects encountered higher false match rates at an ID Key size of 56 bytes than at an ID Key size of 25 bytes.

ID	standard FM	107 FM	56 FM	25 FM	12 FM	Comparisons	standard FMR	107 FMR	56 FMR	25 FMR	12 FMR
861	49	54	54	49	40	1217	4.03%	4.44%	4.44%	4.03%	3.29%
931	32	42	42	25	20	1217	2.63%	3.45%	3.45%	2.05%	1.64%
77	22	36	36	30	14	1217	1.81%	2.96%	2.96%	2.47%	1.15%
264	22	26	26	30	33	1217	1.81%	2.14%	2.14%	2.47%	2.71%
419	27	34	34	25	12	1217	2.22%	2.79%	2.79%	2.05%	0.99%
504	24	26	26	17	29	1217	1.97%	2.14%	2.14%	1.40%	2.38%
167	17	19	19	22	40	1217	1.40%	1.56%	1.56%	1.81%	3.29%
738	22	33	33	23	4	1217	1.81%	2.71%	2.71%	1.89%	0.33%
233	22	31	31	12	19	1217	1.81%	2.55%	2.55%	0.99%	1.56%
884	19	29	29	18	20	1217	1.56%	2.38%	2.38%	1.48%	1.64%

Figure 74: Test Subjects with Highest Aggregated False Match Rates

The distribution of false match rates across all Test Subjects is shown in Figure 75.
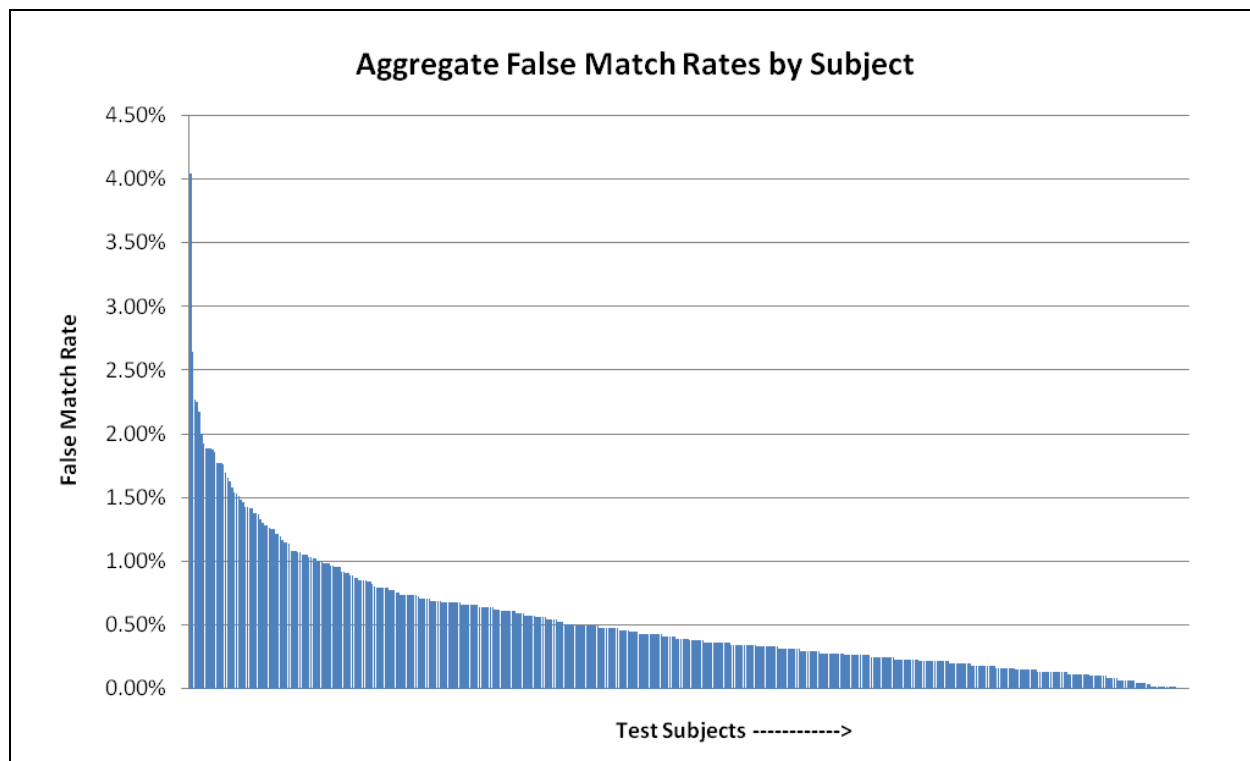
Figure 75: Test Subjects with Highest Aggregated False Match Rates

Annex A   Review of Commercial PET Techniques

A.1   Hitachi, Ltd.

Hitachi, Ltd., Systems Development Laboratory is investing in the research and development of cancelable biometric systems. Hirata and Takahashi (2009) proposed a method that uses correlation-invariant random filtering. The method performed accurately in empirical tests on fingerprint and finger vein verification applications. It is feasible that this protocol was integrated with VeinID, which is reportedly capable of producing encrypted and cancelable biometrics.

VeinID

VeinID is the Hitachi's premier finger vein sensing product. In a presentation by a researcher at the Systems Development Lab, VeinID has been integrated with systems compliant with international standard ITU-T X.1088, which describes standard methods for biometric template protection. According to the presenter, Hitachi deployed VeinID to authenticate users in a Japanese cloud computing service. For each transaction the user presents a finger to a vein sensing device. Vascular patterns are extracted and transformed by a secret parameter. Templates are matched in the encrypted domain. A template can be cancelled by reenrolling a finger vein pattern with a new secret parameter. Upon reenrolling a template, the vascular pattern is encrypted twice: once by the old parameter and once by the new parameter. The difference value between these is sent to the server, where the old template is compared with the difference value. If there is a match, the new template is stored in the dataset.

Hitachi partnered with Medibase to develop BASEmetric, an access control system that is intended to verify and identify patients in health care systems. The system uses VeinID to capture and process finger vein images. A whitepaper of the system claims that it "retains only a mathematical code for identification purposes. The actual finger vein itself is not stored. The mathematical code that is retained is not useful to any entity outside the immediate healthcare system." A press release published in June 2010 reported that BASEmetric had been deployed at two hospitals in an Ohio health system. The publication touts the privacy-preserving characteristics of the system.

Further Reading

Hirata, Shinji. 2009. "Cancelable Biometrics with Perfect Secrecy for Correlation-Based Matching." Hitachi, Ltd., Systems Development Laboratory. "http://www.hitachi.com/rd/sdl/conf/2009/icb/index.html.

Isobe, Yoshiaki. 2010. "Telebiometrics, and Applications in Japan."ITU-T Workshop on Addressing Security Challenges on a Global Scale. http://www.itu.int/dmspub/itu-t/oth/06/35/T063500000200524PDFE.pdf.

Hitachi America, Ltd. 2010. "Hitachi America, Ltd And Medibase Solutions, Inc Deploy Finger Vein Biometric Solution At Health Care System In Ohio." http://www.hitachi.us/about/press/details/063020102.html.

Medibase. "BASEmetric: Accurate Biometric Identification of Returning Patients." http://www.medibase.com/pdf/BASEmetric.pdf.

A.2   Mitsubishi Electric Research Laboratories (MERL)

MERL began investing in the research and development of biometric template protection algorithms circa 2005. Its researchers pioneered the development of syndrome coding methods that employ local aggregation to generate binary feature vectors. The company was the assignee to a patent that laid claim to a method of biometric template protection by way of syndrome coding.

A.3   Securics, Inc.

Securics, Inc. sells products and integrates systems using the biotoken method developed by **Boult et al. (2007)**. The company developed an application for PayPal. It integrates a biometric key infrastructure based on Biotope. Fingerprint data, transactional data, and multiple keys are used to produce private tokens that

protect privacy and security in electronic commerce. After enrollment, users need only to present their fingerprint to confirm a transaction. The fingerprint image is never stored or transmitted. The identity verification process is asymmetric.

A.4   TÜBITAK-UEKAE

The National Research Institute of Electronics and Cryptology (TÜBITAK-UEKAE) is deploying a biometric civil identification system for the Electronic Identity Authentication and Management System in Turkey. The project is expected to be complete in 2013. The new system will feature smart cards that store fingerprint or finger vein data of the card owner. The institute is conducting joint studies with Hitachi-Omron to integrate finger vein recognition into the passport system. A presentation by lead developer Alper Kanak describes the template protection process. During enrollment a biometric input is captured and preprocessed. Features are extracted and scrambled with chaff data generated by a "hardware-based truly random number generator." Genuine and chaff points are represented as triplets (x, y, θ), where x, y are the coordinates of the minutiae points and θ is the angle of the minutiae point. The hardened template is encrypted with a private key and stored on the EEPROM of the smart card, and nowhere else. In a demonstrative presentation of the system the developers reported to have achieve 1.37% EER. Superior results were reported in Kanak and Sogukpinar (2007), which achieved 0.0% FRR at 0.1% FAR.

Annex B   Patent Reviews

B.1   Bjorn (2000)

Assignee: DigitalPersona, Inc.

Bjorn patented a method and apparatus for generating cryptographic keys and digital certificates using fingerprint feature data. This publication was among the first in both academic and commercial discourses to propose the use of biometrics in the key generation process. The proposed method begins with the user presenting a fingerprint image from which features are extracted and encoded onto a template. The template is hashed to create a cryptographic key that is stored on a dataset. In a second proposed variation, additional features are added to the template prior to hashing it. In a third proposed variation, "ghost" features are added to the template prior to hashing it. In the digital certificate variation, the user submits a fingerprint template to a certifying authority (CA). The CA generates a digital certificate that includes the template data and signs the certificate with a private key. The certificate is returned to the user, who decrypts the certificate with the CA's public key. The user retrieves the public key and fingerprint template from the certificate. The user will be able to decrypt a protected file if the public key decrypts the file and the fingerprint matches the template.

B.2   Bolle et al. (2004)

Assignee: IBM Corporation

Bolle et al. were among the first to patent a cancelable biometric authentication system and method.[88] The proposed invention was intended to fortify biometric templates against unauthorized dissemination or theft, which would otherwise permanently compromise the identities of their genuine owners. The principal claim of the invention was the use of parameterized, noninvertible transforms to distort an acquired image or set of features into an encrypted template that cannot feasibly be reconstructed into the original biometric. They extend their claim where: (a) the biometric modality includes a fingerprint, face, hand, iris, blood vessel pattern, vocalization, or signature; (b) the distortions are applied to an orthogonal Cartesian grid or a circular polar-coordinate grid; (c) the distortion process is of a geometric, quantized or block-scrambling nature; (d) the biometric features distorted include fingerprint minutiae, location of facial features, iridial texture, formant frequencies and derivatives of a speech signal, and joint lengths and widths of a hand; (e) the matching process incorporates multiple identifiers. In sum the patent laid claim to most of the fundamental methods that would be used by the researchers whose approaches to cancelable biometrics are reviewed in this report.

B.3   Davida and Frankel (2010)

Davida and Frankel patented a system and method for preserving privacy in biometric authentication and identification systems where the biometric is not stored on a dataset and matching is conducted offline on the client machine. The inventors note that the proposed system could be extended to online systems. On the client machine, only an "identity verification template" (IVT) is stored. The bulk of the patent describes a system for storing and matching biometric templates in a physically and logically secure location. Section 3.2 describes the systemic design of cancelable, multifactor biometric key generation.

B.4   Chang et al. (2010)

Assignee: Industrial Technology Research Institute

Chang et al. patented a system and method for generating cryptographic keys from biometric data by way of feature transformation. Each user possesses a unique transform unit that can be reissued in the event that the protected template is compromised. The inventors mentioned that linear discriminant analysis produces vectors with high interclass variability and low intraclass variability. Thus in a description of the preferred embodiment they explained

---

[88] They filed the patent application in June, 2000, which predates almost all of the articles reviewed in this report.

how to use cascaded linear discriminant analysis, an iterative series of linear discriminant analyses, to map a biometric feature signal onto a projection vector. The optimal projection vector can be derived such that

$$w = \frac{S_w^{-1}(m_a - m_t)}{\|S_w^{-1}(m_a - m_t)\|}$$

where $S_w^{-1}=0.5(S_a + S_t)$, in which S_a and S_t are the covariance matrices of the features of the genuine and imposter users respectively, and m_a and m_t are the mean of biometric features of the authenticated and imposter users respectively. This equation projects high-dimensional biometric features onto a one-dimensional feature space. Iterating the equation M times produces M projection vectors to transform N-dimensional biometric features into M-dimensional feature signals. This process maximizes the distance between the mean samples of an authenticated user and imposters, making each protected template maximally unique relative to one another.

A key generation unit produces a cryptographic key according to bit information stability provided by feature signals in each dimension according to different distinguishabilities. Figure 76 illustrates the procedure for generating reliable cryptographic keys from the feature signal: (a) represents the feature signal distribution of the authenticated user and the global feature signal distribution all users in a given dimension; (b) represents the position of the left and right boundaries JB and RM, expressed as

$$LB = \min\big((m_g - k_g\sigma_g), (m_a - k_a\sigma_a)\big), \text{ and}$$

$$RB = \max\big((m_g - k_g\sigma_g), (m_a - k_a\sigma_a)\big)$$

where m_a and σ_a are the mean and standard deviation of the genuine feature signal distribution and m_g and σ_g are the mean and standard deviation of the global feature distribution; (c) represents the segments with the same size as the authentic region covering the range between the left and right boundaries LB and RM; and (d) represents corresponding index to each above segment, where the index of each segment is selected according to the position of each segment in the feature space.
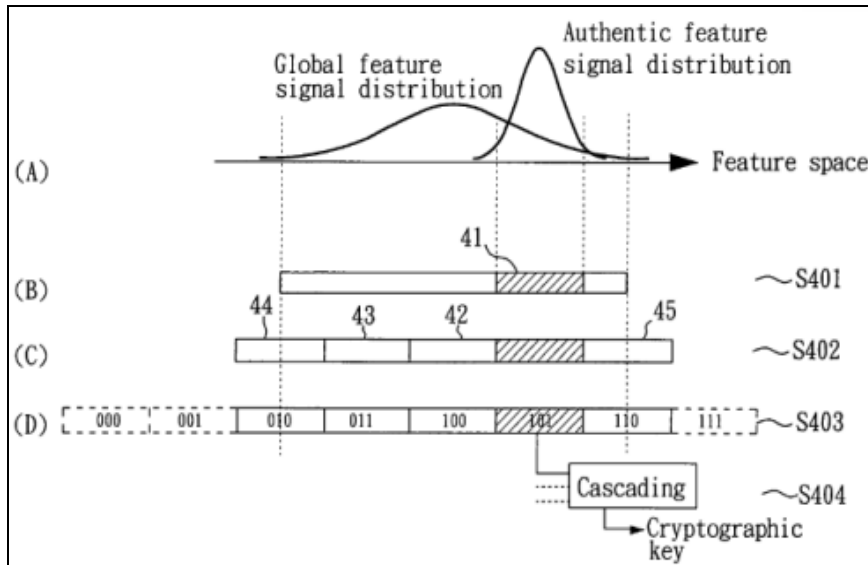
Figure 76: Schematic drawing of the processing procedure of the stable key generation unit

B.5 Draper et al. (2010)

Assignee: Mitsubishi Electric Research Laboratories, Inc.

Draper et al. patented a method for secure biometric data by encoding syndrome vectors. They laid claim to methods

in which a syndrome decoder: (1) uses belief propagation; (2) is based on a measurement model accounting for noise; and (3) determines parameters of source and channel models from training data. The patent mostly describes the preferred embodiments of the proposed method, which include: a syndrome encoder and hashing method for securely storing biometric parameters; a syndrome code based encryption method for securely storing data encrypted with biometric keys; and a method of optimizing syndrome codes used for secure biometric applications. The first is embodiment reviewed in this report.

Syndrome and Hashing Method for Secure Biometric Parameters[89]

During enrollment, the user presents a biometric image from which a feature vector is extracted using an existing feature extraction algorithm. Biometric parameters of the feature vector are encoded using a syndrome encoder; while a message authentication code or hash function is concomitantly applied to the biometric parameters to produce an enrollment hash. The syndrome vector and hash are stored as a pair (S, H) in a dataset. The proposed syndrome encoder can operate on integer values in addition to binary values. During authentication, the parameters of a biometric query are combined with one or more stored syndrome vectors using a syndrome decoder to recreate the parameters of the original biometric. Access is granted if the parameters of the query biometric match those of the decoded biometric. Figure 77 illustrates the systemic design of the patented syndrome and hashing method for biometric template protection.
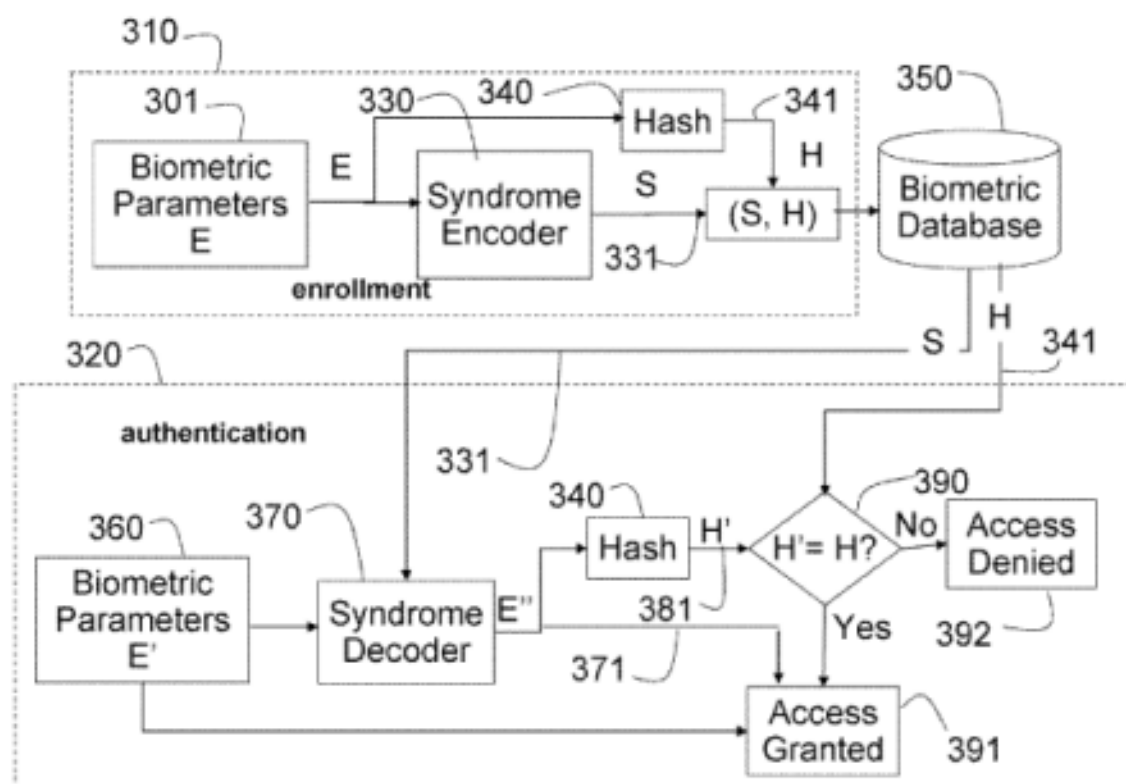
Figure 77: Schematic of a preferred embodiment of a secure biometric access control system

B.6 Akkermans et al. (2007)

Assignee: Philips

Akkermans et al. filed a patent application for the invention of a method and system of protecting templates in biometric identification systems. The explicit goal of the invention was to preserve verification performance while obfuscating the identities of template owners. During enrollment, the user presents multiple impressions of the same

---

[89] See p. 27.

biometric image. Features are extracted from each input image and the elements in the each vector are quantized. The quantized templates are compared, and the components which appear less frequently are considered unreliable and discarded, resulting in a set of reliable feature components likely to be reproduced by the genuine user in subsequent transactions. A subset W1 of the reliable components is stored in a central dataset to be used as helper data during authentication. The security of the system is a function of the value of the quantization resolution, whereby a lower resolution increases the tolerance of the system while increasing the likelihood that an imposter will be incorrectly authenticated. In Section [0021] the inventors extended the preferred embodiment to create cryptographically secure codeword of the biometric data. A randomly generated secret S is encoded into a codeword C and combined with the reliable feature component vector X' by way of, for example, an XOR operation, producing a second helper data set W2. The original secret S is concealed by a hash function F, and both the hashed secret F(S) and the helper data set W2 are stored on the central dataset.

B.7 Bolle et al. (2009a)

Assignee: IBM Corporation

This patent application laid claim to a method whereby an identity is verified or identified upon the successful comparison of two or more encrypted, cancelable biometric templates, such that the identities of the authenticating user and those in the dataset are never disclosed during the whole process of authentication. The process by which templates are matched is as follows: (1) a transformed biometric is presented; (2) a second biometric is transformed in a manner parallel to that of the first biometric; (3) the two transformed biometrics are compared; and (4) matches are reported. Also claimed in the patent are an electronic device and a computer program that execute the proposed method.

Annex C   Iris Recognition Techniques and Standards

C.1   Algorithms and Templates

Iris recognition refers to the process of identifying or authenticating individuals based on random patterns of their irises. Despite its wide employment, automated iris recognition is relatively young. Generally, an iris recognition system is comprised or four steps namely, image capturing, iris segmentation, feature extraction and matching.

The goal of image capturing is to acquire high quality data that is employable for recognition purposes. The purpose of the second step, iris segmentation, is to isolate the iris from the rest of the eye image and the pupil. Segmentation is very important and directly affects the efficiency of feature extraction. There are a number of challenges in localizing the iris such as eyelid and eyelash occlusion, light reflections or shadows created during image capturing.

Feature extraction operates on segmented iris images, for the design of discriminative features i.e., features which are unique to an individual and allow the system to distinguish him/ her in a population. Typically, such features are either texture based or zero crossing representations of concentric circles around the iris. The most widely explored approach to feature extraction is by Daugman [7-11]. However there exist a number of alternative methods that have demonstrated promising results as well. This section provides an overview of these methodologies, along with Daugman's approach and concludes with the related to iris recognition standards currently in place.

Ma et al. [1], proposed a four step recognition algorithm that performs the following operations: Image quality assessment and selection, preprocessing, feature extraction and matching.
A typical iris camera provides more than one snapshots of the iris and the objective is to automatically detect whether the biometric information is occluded, blurred or out-of-focus. A quality descriptor based on the frequency distribution of the captured image is defined as follows:

$$D = \left[(F_{low} + F_{middle} + F_{high}); \frac{F_{middle}}{F_{low} + F_{high}} \right] \tag{1}$$

$$F = \iint_{\Omega = \{(u,v)|f_1 < \sqrt{u^2+v^2} <= f_2\}} | F(u,v) | \, du dv \tag{2}$$

Where $F(u,v)$ is the Fourier spectrum of an iris region and f_1, f_2 are the radial frequency pair and bound the range of the corresponding frequency components (low, middle and high). Every quality factor D has two measures. The first measure can be used to detect occlusion, as it relates to the overall power of the image. The second measure takes smaller values for defocused or blurred images.

Preprocessing is an essential step for biometric recognition systems. Without any treatment, feature extraction from raw images would be meaningless. In [1], preprocessing includes: iris localization, normalization and enhancement. The iris is localized with the Canny edge detector which is applied on the image after projection on the horizontal and vertical directions. The iris is unwrapped to a rectangular block of fixed size with the following transformation:

$$I_n(X,Y) = I_o(x,y) \tag{3}$$

$$x = x_p(\theta) + (x_i(\theta) - x_p(\theta))\frac{Y}{M} \tag{4}$$

$$y = y_p(\theta) + (y_i(\theta) - y_p(\theta))\frac{Y}{M} \tag{5}$$

$$\theta = \frac{2\pi X}{N} \tag{6}$$

Where I_n is the image, $(x_p(\theta), y_p(\theta))$ and $(x_i(\theta), y_i(\theta))$ are the coordinates of the inner and outer boundary points in the direction θ in the original image I_o. Finally, an estimate of the background illumination is used to adjust the contrast of the image so that the texture if uniformly enhanced along the rectangular.

Feature extraction in [1] operates in the frequency domain, with the use of circularly symmetric sinusoidal functions. These functions are similar to Gabor filters with the difference being that the latter use oriented sinusoidal functions. The kernels of the filters applied in [1] target to capture the local properties of the texture and are estimated as follows:

$$G(x, y, f) = \frac{1}{2\pi\delta_x\delta_y}\exp\left[-\frac{1}{2}\left(\frac{x^2}{\delta^2_x} + \frac{y^2}{\delta^2_y}\right)\right]M_i(x, y, f), \quad i = 1, 2 \tag{7}$$

$$M_1(x, y, f) = \cos(2\pi f(\sqrt{x^2 + y^2})) \tag{8}$$

$$M_2(x, y, f) = \cos(2\pi f(x\cos\theta + y\sin\theta)) \tag{9}$$

Where $M_i(x, y, f)$ denotes the modulating sinusoidal function, f is the frequency of the sinusoidal function and δ_x, δ_y are the space constants of the Gaussian envelope along the x and y axis respectively and θ denotes the orientation of the Gabor filter.

It was observed that the upper portion of the normalized iris image (closer to the pupil) provides the most distinctive texture information. Furthermore, there are lower chances of eyelashes to occlude these regions. For this reason, only this region of interest (ROI) was used for feature extraction. Given the above specified filters, the output of feature extraction is:

$$F_i(x, y) = \iint I(x_1, y_1)G(x - x_1, y - y_1)dx_1dy_1, \quad i = 1, 2 \tag{10}$$

Where G_i is the ith channel of the spatial filters, $I(x, y)$ denotes the ROI and $F_i(x, y)$ is the filtered image. In addition, statistical features are extracted for each 8x8 block. For every filtered block the mean and the absolute deviation serves as the feature vector:

$$m = \frac{1}{n}\sum_w |F_i(x, y)| \tag{11}$$

$$\sigma = \frac{1}{n}\sum_w ||F_i(x, y)| - m| \tag{12}$$

Where w is an 8x8 block in the filtered image and n is the number of pixels in that block. Such features acquired from all the respective blocks in the ROI are concatenated into an 1D feature vector. Therefore, the output of feature extraction is a feature vector of length 1536.

The dimensionality of the feature vector is reduced prior to classification. This reduction was based on the Fisher Linear Discriminant Analysis (LDA), which is a supervised machine learning technique. LDA transforms a vector in a way that the within-subject variability is reduced and at the same time the between-subject is augmented. Given an LDA transformation matrix W, the new feature vector is estimated through projection:

$$f = W^T V \tag{13}$$

Where V is the 1536 dimensional input, and f is the new feature vector of reduced dimensionality. Classification is performed based on the nearest centre method, with the Euclidean norm utilized as the similarity measure.

The system in [1] was tested on the CASIA Iris dataset, which includes 2255 iris images from 213 subjects. The performance was reported for various dimensionalities of the feature vector, with accuracy reaching 99.43% for a dimensionality of 220.

Boles et al. [2] proposed a feature extraction scheme based on the wavelet transform of the iris signature i.e., the gray scale density along concentric contours. The essence of the feature extractor lies on the local structure of the iris patterns along circles. More specific, the proposed framework is comprised of three steps, namely preprocessing, feature extraction and classification.

During preprocessing is the image is subjected to edge detection for the localization of the iris. By taking into consideration the fact that iris has a circular shape, edge detection is tuned in seeking a closed contour.

The region formed by the circular contour propagates to feature extraction. Since the local structure is examined at a circular level, a reference point is determined based on the centroid of the previously detected iris. Using this point, a number of virtual contours are considered to be structurally circular and concentric around the pupil. Every contour is revisited and treated independently by feature extraction as an 1D signal. The amplitude along the contour (gray scale intensity) is normalized and the length is normalized to acquire comparable views for any image. The 1D signal is further processed using the dyadic wavelet transform, in order to retain only few low resolution levels not affected by high frequency noise. The zero crossings along these levels are detected and used for the design of the biometric template.

The template is a combination of both the location of the zero crossings and the amplitude of the signal between two adjacent zero crossings. For instance, at a particular wavelet level j the template, denoted as $Z_j f$, is a set of ordered complex numbers for which the real part describes the magnitude between two adjacent zero-crossings, and the imaginary part the locations of the zero-crossings.

For matching, two dissimilarity measures are defined to associate an unknown input signature g and candidate identity f at a particular resolution level j :

$$d^{(1)}{}_j(f,g) = \min_m \sum_{n=1}^{N} | Z_j f(n) - \Gamma Z_j g(n+m) |^2 \qquad (14)$$

$$d^{(2)}{}_j(f,g) = \min_m \frac{\sum_{r=1}^{R_j} \left\{ [\mu_j(r)]_f [\rho_j(r)]_f - \Gamma[\mu_j(r+m)]_g [\rho_j(r+m)]_g \right\}^2}{\Gamma \sum_{r=1}^{R_j} | [\mu_j(r)]_f [\rho_j(r)]_f [\mu_j(r)]_g [\rho_j(r)]_g |} , \quad m \in [0, R_j - 1] \quad (15)$$

Where Γ is a scale factor, while $[\mu_j(r)]$ and $[\rho_j(r)]$ are the real and imaginary parts of the representation respectively. The overall dissimilarity of g and f is the average dissimilarity of the two over all decomposition levels.

The performance of this algorithm was reported for iris images of two subjects but under lighting and noise variations as well as for different camera-to-face distances. The proposed dissimilarity measures managed to distinguish the two irises even under extreme lighting and distance variations. However, the system was shown to be prone to noise.

Wildes et al. [3] were among the earliest to explore automatic iris recognition. Apart from the template design algorithm, this work also presented a schematic diagram for the acquisition of the iris image, by taking into account the effects of illumination as well as the positioning of the eye into the camera's field of view. Preprocessing of the acquired image included simple low-pass filtering with a Gaussian filter, and spatial down-sampling that reduces the resolution in order to better assist iris detection. The iris is then localized using gradient-based edge detection and

simple voting of the detected edge pixels. The essence of feature extraction in [3], was to capture the range of spatial structures using a two-dimensional band-pass decomposition. The decomposition was based on a Laplacian pyramid. A four level decomposition was performed, where every level encompassed two steps:

- Low pass filtering of the iris and down-sampling by a factor of two on the horizontal and vertical directions.

- Starting from the smallest image, it is expanded by a factor of two (up-sampling with linear interpolation) and subtracted from the one which is one level below.

With this expansion, four band-pass iris images were acquired and used as the biometric template. Matching was performed using a shift, scale and rotate methodology which given a pixel at the template image seeks to establish a match with any pixel of the input image.

The performance of this algorithm was tested on 500 iris images from 50 volunteers. Impostor tests were performed using 40 of those subjects. The identification performance was 100%.

Avila et al. [4] presented a zero-crossing based iris representation in 2002. The first step of the algorithm was to convert the color image to gray scale and to normalize the respective histogram. Iris localization was then performed by locating the centre of the iris as well as by taking advantage of the circular structure. Furthermore, the diameter of the iris was normalized, to acquire comparable irises along all images. However, no other information was reported on this process.

Feature extraction was based on the gray color intensity along virtual co-centered contours, using the centre of the pupil as a reference. This is essentially a 256bits 1D signal, referred to as the iris signature. Once the signature was acquired, the dyadic wavelet transform was used for further processing and template design.

The signal at every level was searched for sign changes. Linear interpolation was used between consecutive samples of opposite signs, in order to establish the location of zero-crossings. Only the finest levels of the decomposition were excluded from this process, due to their vulnerability to high frequency noise (only the four lowest levels were used for matching).

Matching was performed using three different measures i.e., the Euclidean distance, the Hamming distance and dissimilarity functions. The Hamming distance was observed to achieve the highest classification rate (97.9%) for 200 images of 20 subjects.

An approach based on Gabor filtering and the wavelet transform was reported by **Zhu et al. [5]**. Similar to other methodologies, preprocessing was a three step operation as follows:

- Iris localization, where the geometrical and color information of the pupil is used to isolate it.
- Iris normalization that accounts for the possible deformations, by mapping the iris to a rectangular block of fixed size.
- Image enhancement with local histogram normalization. This operation treats the effects of non uniform illumination.
- Feature extraction encompassed two sets of features, both related with the texture of the iris. First, a multi-channel Gabor filter was designed for every cortical channel:

$$h_e(x, y) = g(x, y)\cos[2\pi f(x\cos\theta + y\sin\theta)]$$

(16)

$$h_o(x, y) = g(x, y)\sin[2\pi f(x\cos\theta + y\sin\theta)]$$

(17)

Where $g(x, y)$ is a 2D Gaussian function while f and θ are the central frequency and the orientation that define the location of the channel in the frequency plane. For every central frequency (power of 2), filtering is performed for various angles θ, this way resulting into a number of images. The feature vector is then the concatenation of the means and standard deviations for all images. Similarly, the mean and standard deviation of five low resolution levels acquired using the 2D wavelet transform are used for matching.

The Euclidean distance is used to associate an input and a pre-enrolled iris, at the matching stage. This system was tested on 160 iris images from 16 different subjects. The overall recognition rate was 93.8%.

In 2001 **Lim et al. [6]** proposed an improvement on prior feature extraction methodologies with the use of the 2D Haar wavelet for the exploration of texture characteristics of the iris. A preprocessing stage performed operations such as iris localization and normalization. Localization was based on edge detection and normalization was suggested by fixation of the distance between the detected inner and outer boundaries of the iris.

The preprocessed image is decomposed four times with the Haar transform, and features are selected from the high pass sub-bands (HH4, HH3, HH2 and HH1). More specific, the HH4 sub-band was retained for classification while only the average was used for sub-bands HH3, HH2 and HH1. To control space and computational effort, the feature vector was quantized into binary values via a simple sign rule i.e., positive values were represented by 1 while negative by 0.

For classification, a competitive neural network was proposed (LVQ). The reason for this choice was that, compared to other leaning networks, LVQ is faster in training. However, the performance of the LVQ is prune to initial weight vectors. To address this problem, the authors of [6] proposed a novel initialization process by which initial vectors are located at the boundaries of each class.
The performance of the proposed system was tested on 6000 iris images from 200 volunteers. The overall recognition rate achieved was 99.3%.

The most widely deployed algorithm for iris recognition was proposed by **Daugman [7-11]** based texture characteristics of the iris, explored through a 2D wavelet decomposition procedure.

The preprocessing step of Daugman's algorithm includes image focus assessment and iris localization. In order to determine if the image is usable for feature extraction, the spectral power in the middle and upper frequency bands of the 2D Fourier transform is examined. This assessment is rather performed during the acquisition stage, where the goal is to acquire an image for which these quantities are maximized.

Daugman also proposed a very effective operator that can be used to determine the boundaries of the iris and pupil. As opposed to other works, this operator does not assume that circular contours which surround these regions are concentric, and because of this the parameters of the two circles were defined separately. For an image $I(x, y)$, the operator is defined as follows:

$$\max_{(r,x_o,y_o)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_o,y_o} \frac{I(x,y)}{2\pi r} ds \right|$$

(18)

Where $G_\sigma(r)$ is a smoothing function such as a Gaussian of scale σ. Essentially, this operator behaves as a circular edge detector that localized both the iris and the pupil.
For feature extraction Daugman [7] proposed a 2D wavelet demodulation algorithm. More specific, the proposed wavelets were Gabor filters:

$$G(x, y, f) = \frac{1}{2\pi\delta_x\delta_y} \exp\left(-\frac{1}{2}\left(\frac{x^2}{\delta^2_x} + \frac{y^2}{\delta^2_y}\right)\right) \cos(2\pi f(x\cos\theta + y\sin\theta))$$

(19)

Where f the frequency of the sinusoidal is function, δ_x and δ_y are the space constants of the Gaussian envelopes and θ is the orientation of the Gabor filter.
The encoding is essentially a phase quantization procedure which identifies in which quadrant of the complex plane each phasor lies. Encoding can be described through:

$$h_{\{\mathrm{Re,Im}\}} = \mathrm{sgn}_{\{\mathrm{Re,Im}\}} \int_{\rho} \int_{\varphi} I(\rho, \varphi) e^{-i\omega(\theta_0 - \varphi)} \, e^{\frac{-(r_o - \rho)^2}{a^2}} \, e^{\frac{-(\theta_0 - \varphi)^2}{\beta^2}} \, \rho \, d\rho \, d\varphi$$

$$(20)$$

Where $h_{\{\mathrm{Re,Im}\}}$ is a complex valued bit is whose real and imaginary parts are either 1 or 0 depending on the sign of the integral. α and β are the multiscale wavelet size parameters, and (r_o, θ_0) represent the polar coordinates of each region of the iris for which the phasor coordinates $h_{\{\mathrm{Re,Im\}}}$ are computed. In total, 2048 phase bits (iris code) are computed for each iris.

A test of statistical independence was also proposed by the same author that estimates the similarity (or difference) between two 2048 bit streams. This test is based on simple XOR operations that return 1 if the two bits under consideration are different.

In addition to the iris code, each iris is accompanied by a mask of the same length that signifies parts which parts of the code represent occlusion information. The goal is to test independence without taking into account occluded portions of the iris.

For two iris codes $codeA$ and $codeB$, and for the respective masks $maskA$ and $maskB$ the following measure of dissimilarity was proposed by Daugman [7]:

$$HD = \frac{\lVert (codeA \otimes codeB) \cap maskA \cap maskB \rVert}{\lVert maskA \cap maskB \rVert}$$

$$(21)$$

Which is the Hamming distance, a well known measure of dissimilarity between two binary streams. The HD between two iris codes from different subjects should be normally distributed with a mean of 0.5. HDs from comparison of 4258 different iris images were computed (over 9.1 million comparisons) from individuals in the U.K., U.S.A., Japan and Korea. The observed mean HD was 0.499 with a standard deviation of 0.0317. Figure 78 provides a comparison of the above mentioned approaches with respect to preprocessing, feature extraction, classification algorithms and performance.

		Ma et al. [1]	Boles et al. [2]	Wildes et al. [3]	Avila et al. [4]	Zhu et al. [5]	Lim et al. [6]	Daugman [7]
Preprocessing		Quality assessment Iris localization Iris normalization	Iris localization	Low pass filtering Iris localization	Histogram normalization Iris localization	Iris localization Iris normalization Image enhancement	Iris localization Iris normalization	Focus assessment Iris localization with circular edge detection
Iris Template	**Template Type**	Texture based	Zero-crossing representation	Texture based	Zero-crossing representation	Texture based	Texture based	Texture based
	Feature Extraction	Localized spatial filters on regions close to the pupil	Wavelet transform	Decomposition using a Laplacian pyramid	Wavelet transform on co-centered contours.	Gabor filters and wavelet transform	Haar wavelet transform	2D wavelet demodulation
Feature Selection		Linear Discriminant Analysis	Zero crossings at low resolution decomposition levels and intermediate magnitude.	Band-pass difference images from the various decomposition levels.	Location of zero crossings at low resolution levels.	Mean and standard deviation	Winner selection	2048 phase bits
Classification		Nearest centre based on Euclidean norms.	Dissimilarity measures	Pixel mapping function	Euclidean distance Hamming distance Dissimilarity functions	Euclidean distance	Competitive learning neural network	Measure of statistical independence
Performance	**Number of iris images**	2255	4	500	200	160	6000	4258
	Number of subjects	220	2	50	20	16	200	4258
	Accuracy	99.43%	100%	100%	97.9%	93.8%	99.3%	HD=0.499

Figure 78: Comparison of iris recognition algorithms

C.2　　　　Iris Recognition Standards

ISO/IEC 19794-6: 2005 Biometric data interchange format - Part 6: Iris image data specifies two alternative image interchange formats for biometric authentication systems that utilize iris recognition. The first is based on a rectilinear image storage format that may be a raw, uncompressed array of intensity values or a compressed format such as that specified by ISO/IEC 15444. The second format is based on a polar image specification that requires certain pre-processing and image segmentation steps, but produces a much more compact data structure that contains only iris information.

ISO/IEC TR 19795-3: 2007 Biometric performance testing and reporting -- Part 3: Modality-specific testing describes the methodologies relating to these modality-dependent variations. It presents and defines methods for determining, given a specific biometric modality, how to develop a technical performance test. In biometric performance testing and reporting, careful consideration needs to be given to the characteristic differences of each modality (fingerprint, face, iris, etc.). These differences naturally require variations within the general methodology defined in ISO/IEC 19795-1. ISO/IEC TR 19795-3:2007

NISTIR 6529-A Common biometric exchange formats framework (CBEFF) relates to all biometric modalities. It describes a structure and set of metadata elements necessary to support exchange of biometric information in a common way.

ANSI INCITS 358-2002 [2007] (Initially developed by the BioAPI Consortium, Reaffirmed 2007) - American National Standard for Information technology for Information Technology – The BioAPI Specification specifies the Application Programming Interface and Service Provider Interface for a standard biometric technology interface. It is beyond the scope of this specification to define security requirements for biometric applications and service providers, although some related information is included by way of explanation of how the API is intended to support good security practices. The BioAPI is intended to provide a high-level generic biometric authentication model; one suited for any form of biometric technology. The standard covers the basic functions of Enrollment, Verification, and Identification, and includes a dataset interface to allow a biometric service provider (BSP) to manage the Identification population for optimum performance. It also provides primitives that allow the application to manage the capture of samples on a client, and the Enrollment, Verification, and Identification on a server.

ANSI INCITS 398-2008 (Revision of ANSI INCITS 398-2005) American National Standard for Information Technology – Common Biometric Exchange Formats Framework (CBEFF) specifies a common set of data elements necessary to support multiple biometric technologies and to promote interoperability of biometric-based application programs and systems by allowing for biometric data exchange. This standard (revision of ANSI INCITS 398-2005) specifies a common set of data elements necessary to support multiple biometric technologies and to promote interoperability of biometric-based application programs and systems by allowing for biometric data exchange. These common data elements can be placed in a single file, record, or data object used to exchange biometric information between different system components and applications.

This standard specifies the biometric data elements. These elements are assembled into data structures defined by CBEFF patron format specifications or standards. Each patron format specification that conforms to CBEFF defines which CBEFF data elements are present in its format and how the data elements are extracted and processed (details such as the data encoding scheme are the responsibility of the CBEFF patrons). The biometric data transported in a CBEFF structure can represent processed or unprocessed (raw) data. This standard itself specifies two Patron Formats (Patron Format A and B, see Annexes A and B). Annexes C through F document patron formats that have been specified external to this standard, as follows: C. The BioAPI BIR, D. The NIST PIV CBEFF Patron Format specified in NIST SP 800-76, Feb 1, 2006, E. The ICAO Logical data Structure (LDS), F. The Type 99 record specified in the revision of the ANSI/NIST-ITL 1-2000 standard (ANSI/NIST-ITL 1-2007, "Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information"). CBEFF does not specify the content or format of the actual biometric data contained within a CBEFF biometric data record. Protection of the privacy of individuals from inappropriate dissemination and use of biometric data is not in the Scope of this standard.

C.3 References

[1] Ma L., Tan T., Wang Y., ZhangD., "Personal identification based on iris texture analysis," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol.25, no.12, pp. 1519- 1533, Dec. 2003

[2] Boles, W.W., Boashash, B., "A human identification technique using images of the iris and wavelet transform," *IEEE Transactions on Signal Processing,* vol.46, no.4, pp.1185-1188, Apr 1998

[3] Wildes R. P., Asmuth J. C., Green G. L., Hsu S. C., Kolczynski R. J., Matey J. R., and McBride S. E., "A machine vision system for iris recognition", *Mach. Vision Applicat.*, vol. 9, pp. 1 - 8, 1996.

[4] Sanchez-Avila C., Sanchez-Reillo R., de Martin-Roche, D. , "Iris-based biometric recognition using dyadic wavelet transform," *IEEE Aerospace and Electronic Systems Magazine* , vol.17, no.10, pp. 3- 6, Oct 2002

[5] Zhu Y., Tan T., Wang Y., "Biometric personal identification based on iris patterns," Proceedings *of 15th International Conference on Pattern Recognition*, vol.2, no., pp.801-804 vol.2, 2000

[6] Lim S., Lee K., Byeon O., Kim T., "Efficient Iris Recognition through Improvement of Feature Vector and Classifier," ETRI Journal, vol.23, no.2, June 2001, pp.61-70

[7] Daugman, J., "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol.14, no.1, pp. 21- 30, Jan. 2004

[8] Daugman, J., "Biometric personal identification system based on iris analysis", U.S. Patent 291560, 1994

[9] Daugman, J., "Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons," *Proceedings of the IEEE* , vol.94, no.11, pp.1927-1935, Nov. 2006

[10] Daugman J., "Demodulation by complex-valued wavelets for stochastic pattern recognition." *Int'l Journal of Wavelets, Multi-resolution and Information Processing,* 1(1), pp 1-17

[11] Daugman J., "The importance of being random: Statistical principles of iris recognition." *Pattern Recognition,* 36(2), pp 279-291

Annex D Fingerprint Recognition Techniques and Standards

D.1 Fingerprint Algorithms and Templates

Feature extraction from fingerprint images may operate on three distinct levels:

Level 1 features describe the overall ridge patterns i.e., the flow and direction of lines in the image. Level 2 fingerprint features are more detailed as they describe the various ridge path deviations such as ridge endings or splits (bifurcation). Accordingly, level 3 fingerprint features describe ridges in even greater detail, using information such as the width, shape, pores and other. All three levels have been explored for biometric recognition, with level 2 being the most widely deployed. For the purpose of this report, feature extraction algorithms are categorized as pattern-based or minutiae-based. Essentially, the first falls under level 1 features, and the latter under level 2. From a pattern recognition point of view, pattern-based approaches process the fingerprint image holistically, while minutiae patterns describe mostly local characteristics.

A great challenge in fingerprint recognition is the design of templates that are robust to elastic distortion. In addition, approaches that rely on minutiae points require perfect sensor readings, otherwise fake minutiae points will be generated by the algorithms.

To address these issues, **<u>Xie et al. [12]</u>** proposed a fingerprint template based on ridge patterns, which means that the fingerprint image can be processed holistically, without the need of minutiae points detection.

The first step in the study of fingerprint patterns is the extraction of the skeleton ridge image out of the raw sensor output. A typical solution is by **<u>Maio et al. [15]</u>**, whereby the progression of a ridge is examined until either a termination of intersection with other ridges. Eventually, a skeleton image is a binary image of lines running along the fingerprint ridges.

Once the skeleton fingerprint is available, the next step is labeling the ridges and examining the global structure. Suppose P_m and P_n are the starting and ending points of an arbitrary ridge f These points can then be either ending points, ridge bifurcations or broken ridges. Xie et al. [12] defined the curvature γ of f as:

$$\gamma = \int_{P_m}^{P_n} | d^2 f |$$

(14)

Therefore γ is a measure of the ridge's winding degree, thus naturally invariant to the image rotation or translation. To associate two ridges f_1 and f_2 of lengths d_1 and d_2 the following conditions are examined:

$$\begin{cases} \left| \dfrac{d_2 - d_1}{d_2} \right| \leq th1 \\ 1 - \left| \dfrac{1-k}{1+k} \right| \left| \dfrac{\gamma_{f_1} - \gamma_{f_2}}{\gamma_{f_1} + \gamma_{f_2}} \right| \geq th2 \end{cases}$$

(15)

$$k = \frac{d_1}{d_2}$$

Where $\dfrac{d_1}{d_2}$ and $th1$, $th2$ are two thresholds. If the above two conditions are satisfied, the ridges under consideration are pre-matched. For every ridge, an associate table is designed by sampling it at a number of points, and associating every point with ridges in the upper and lower parts (using the two conditions). In Xie et al.'s work [12], fingerprint templates are a set of associate tables (one for every ridge), which in combination provide a

structural picture of the fingerprint image.

Marana et al. [13] proposed another ridge based fingerprint template, using the Hough transform. The framework can be described in four steps:

- Design of skeleton image. During this step, a gray scale fingerprint image is converted into a thinned skeleton image (one pixel wide). This is achieved with the estimation of the orientation field and segmentation, as well as several heuristics that remove holes and speckles in the binary ridge map.

- Ridge detection. During this step, the goal is to extract straight lines that approximate the fingerprint ridges. The Hough transform [16] is used to examine each pixel of a given ridge and increment an accumulator bin according to all the possible straight lines that pass through that pixel. The peaks of the accumulator array of pixels belonging to the same ridge indicate the parameters of the most likely straight lines that match that ridge in the image.

- Fingerprint registration. In order to align an input and a gallery fingerprint image, rotation, translation and scale parameters are estimated. If the peak sets from the previous step are denoted as S_I and S_g for the input and gallery images respectively, for every pair of peaks (I_i, G_i) where $I_i \in S_I$ and $G_i \in S_g$ a 1D rotation and a 2D translation parameters are estimated. The scale factor was simply set to 1, since all images were acquired with the same sensor.

- Fingerprint matching. Using every triplet of rotation and translation parameters $(\Delta_g, \Delta_x, \Delta_y)$, the input image is aligned with the template image, and a matching score is calculated. The overall score of the pair is the maximum for all triplets.

The match score is proportional to the number of detected ridges in the input and gallery images. The score is estimated using:

$$s = \frac{2\left(\sum_{i=1}^{n_1}\sum_{j=1}^{n_2} C(i,j)^2\right)}{a+b}$$
(16)

Where the (i,j)-th element of matrix C indicates how many pixels of the i-th ridge of the template fingerprint coincide with pixels of the j-th ridge of the template fingerprint. Also a and b are estimated as:

$$a = \sum_{i=1}^{n_1} (R_I(i)_{nop})^2$$
(17)

$$b = \sum_{i=1}^{n_2} (R_G(i)_{nop})^2$$
(18)

Where $R(i)_{nop}$ is the number of pixels of the i-th ridge of the input fingerprint. Only the ridges of one fingerprint image that intercept at least one ridge of the other image are considered in the computation, because they carry high entropy information.

Khalil et al. [14] proposed a fingerprint verification algorithm based on statistical descriptors. The essence of the method is the statistical analysis of co-occurrence matrices obtained using a singular point on the orientation field. The algorithm is comprised of five steps:

- Image enhancement. The short time Fourier transform is applied on overlapping windows of the fingerprint image for filtering. This analysis outputs the ridge orientation image, the energy image and the ridge frequency image. Then an angular filter is used for enhancement.

- Detection of singular point. To detect this point, the image is divided into non-overlapping blocks of size 16x16. The gradients on the horizontal and vertical directions are computed (using a Sobel mask), denoted as $G_x(x, y)$ and $G_y(x, y)$ respectively. The ridge orientation of every pixel is then computed for the gradients within a window $w \times w$ as

$$G_{xx} = \sum_{(x,y)\in w} G^2_x(x, y)$$

(19)

$$G_{yy} = \sum_{(x,y)\in w} G^2_y(x, y)$$

(20)

$$G_{xy} = \sum_{(x,y)\in w} G_x(x, y)G_y(x, y)$$

(21)

$$\theta(x, y) = \frac{1}{2}\tan^{-1}\left(\frac{2G_{xy}}{G_{xx} - G_{yy}}\right)$$

(22)

The ridge orientation is smoothened with a Gaussian low-pass filter. Next, the orientation image is converted into a continuous vector field as follows:

$$\Phi_x = \cos(2\vartheta(x, y))$$

(23)

$$\Phi_y = \sin(2\vartheta(x, y))$$

(24)

And a two dimensional Gaussian low-pass filter is applied on Φ_x and Φ_y. The singular point, is the point of maximum curvature, and it can be found using

$$\gamma_{min} = \frac{(G_{yy} + G_{xx}) - (\Phi_x G_{xx} - G_{yy}) - \Phi_y G_{xy}}{2}$$

(25)

$$\gamma_{max} = G_{yy} + G_{xx} - \gamma_{min}$$

(26)

$$reliability = 1 - \frac{\gamma_{min}}{\gamma_{max}}$$

(27)

- Extraction of sub-image. The detected singular points acts as the centre for determining a sub-image of size 129x129 from the original fingerprint image.

- Feature extraction. The gray level co-occurrence matrix (GLCM) is then used to extract texture characteristics

from the sub-image. A co-occurrence matrix is specified by the relative frequencies $P(i, j, d, \theta)$ in which two pixels, separated by a distance d, occur in a direction specified by an angle θ, one with gray level i and one with j. Several GLCMs are computed for a number of directions θ and the template is based on four statistical features for every matrix:

Correlation
$$\sum_{i=1}^{k} \sum_{j=1}^{k} \frac{(i - m_r)(j - m_c)P_{ij}}{\sigma_r \sigma_c}$$
(28)

Contrast
$$\sum_{i=1}^{k} \sum_{j=1}^{k} (i - j)^2 P_{ij}$$
(29)

Energy
$$\sum_{i=1}^{k} \sum_{j=1}^{k} P^2_{ij}$$
(30)

Homogeneity
$$\sum_{i=1}^{k} \sum_{j=1}^{k} \frac{P_{ij}}{1 + |i - j|}$$
(31)

Minutiae based approaches to fingerprint recognition are most typical and most widely deployed solutions. As opposed to pattern based approaches that examine the signal holistically and design texture or morphological templates, approaches based on minutiae points explore the finest characteristics of fingerprint images. Among such approaches, **Jain et al. [17]** fingerprint templates became very popular.

A minutiae point can take the form of ridge ending or bifurcation. The location of such points on the fingerprint is what makes this modality unique. However, in order to extract this information there several steps that need to be followed, in order for the image to be appropriately pre-processed i.e., orientation field estimation and ridge detection.

Jain at al. [17] suggested that the orientation field can be estimated in sixsteps as follows:

- Divide the image in blocks of size w.
- Compute the gradients f_x and f_y of each pixel for both directions.
- Calculate the local orientation tables V_x and V_y based on the gradients:

$$V_x = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2G_x(u,v)G_y(u,v)$$
(32)

$$V_y = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} (G^2_x(u,v) - G^2_y(u,v))$$
(33)

Estimate the orientation θ for every wxw block.

$$\partial(i, j) = \frac{1}{2} \tan^{-1} \left(\frac{V_x(i, j)}{V_y(i, j)} \right)$$
(34)

Apply a low-pass filter a block level.
Compute the local ridge orientation O.

Once the orientation field is estimated, a segmentation algorithm is applied to remove the background information of the image. A measure of local certainty is used to locate regions of interest:

$$CL(i, j) = \sqrt{\frac{1}{w \times w} \frac{(V^2_x(i, j) + V^2_y(i, j))}{V_e(i, j)}}$$

(35)

Where

$$V_e(i, j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} (G^2_x(u, v) + G^2_y(u, v))$$

(36)

A threshold on the certainty level $CL(i, j)$ allows the system to distinguish and remove background information which is redundant.

The next step of the algorithm is the detection of pixels that belong to ridges. Detection is based on the gray level intensity of these pixels along a direction normal to the local ridge map. To do that, two masks are defined and convolved with the image:

$$h_t(i, j, u, v) = \begin{cases} -\frac{1}{\sqrt{2\pi}\delta} e^{-\frac{u}{\delta^2}}, & if \quad u = (v \cot(\theta(i, j))) - \frac{H}{2\cos(\theta(i, j))}) \\ \frac{1}{\sqrt{2\pi}\delta} e^{-\frac{u}{\delta^2}}, & if \quad u = u \cot(\theta(i, j)) \\ 0, & otherwise \end{cases}$$

(37)

$$h_b(i, j, u, v) = \begin{cases} -\frac{1}{\sqrt{2\pi}\delta} e^{-\frac{u}{\delta^2}}, & if \quad u = (v \cot(\theta(i, j))) + \frac{H}{2\cos(\theta(i, j))}) \\ \frac{1}{\sqrt{2\pi}\delta} e^{-\frac{u}{\delta^2}}, & if \quad u = u \cot(\theta(i, j)) \\ 0, & otherwise \end{cases}$$

(38)

These masks are able to adaptively identify the local maximum gray-level values along a local ridge direction. If both gray scale intensities are larger than a threshold, then the respective pixel is labeled as a ridge. Once a skeleton image is available, minutiae detection is the last step of the biometric template design. The algorithm for the detection is heuristic. For a pixel at a location (x, y) known to be on a ridge the eight neighbors $N_0, N_1, ..., N_7$ are examined.

$$\left(\sum_{i=0}^{7} N_i \right) = 1 \qquad\qquad \left(\sum_{i=0}^{7} N_i \right) > 2$$

The pixel is classified as ridge ending if $\left(\sum_{i=0}^{7} N_i \right) = 1$ and ridge bifurcation if $\left(\sum_{i=0}^{7} N_i \right) > 2$. However, because this procedure is very sensitive to surrounding spikes due to noise or misinterpretation of pixels, a smoothing operation is first applied on the ridge skeleton to remove rapid spikes and to connect broken ridges. According to [17] the fingerprint template is comprised of the following information for every detected minutiae point:

- Coordinate x
- Coordinate y

- Orientation
- Associated ridge segment

D.2　　　Fingerprint Standards

ANSI/INCITS 381-2004 – Finger image based data interchange format specifies an interchange format for the exchange of image-based fingerprint and palm print recognition data. It defines the content, format, and units of measurement for such information. This standard is intended for those identification and verification applications that require the use of raw or processed image data containing detailed pixel information.

ANSI/INCITS 377-2009 – Finger Pattern Data Interchange Format specifies an interchange format for the exchange of pattern-based fingerprint recognition data. It describes the conversion of a raw fingerprint image to a cropped and down-sampled finger pattern followed by the cellular representation of the finger pattern image to create the finger-pattern interchange data. The main points of difference between this revised version and the original standard are the inclusion of two new fields in the Record Header part of the Finger Pattern Data Record. These new fields are called Capture Equipment Compliance (see 6.2.4.2) and Capture Equipment ID (see 6.2.4.3). The revised standard also describes a method to store (optional) Core and Delta information in the Extended Data field of the Finger Pattern Data record (see 6.3.2.2). The above changes were done to improve the standard's usability from a commercial point of view and also to harmonize it with ANSI INCITS 378-2004, Finger Minutia Format for Data Interchange.

ISO/IEC 19794-2:2005 – Biometric data interchange formats -- Part 2: Finger minutiae data specifies a concept and data formats for representation of fingerprints using the fundamental notion of minutiae. It is generic, in that it may be applied and used in a wide range of application areas where automated fingerprint recognition is involved. ISO/IEC 19794-2:2005 contains definitions of relevant terms, a description of how minutiae shall be determined, data formats for containing the data for both general use and for use with cards, and conformance information. Guidelines and values for matching and decision parameters are provided in an informative annex. ISO/IEC 19794-2:2005 specifies the fundamental data elements used for minutiae-based representation of a fingerprint; three data formats for interchange and storage of this data: a record-based format, and normal and compact formats for use on a smart card in a match-on-card application; optional extended data formats for including additional data such as ridge counts and core and delta location. ISO/IEC 19794-2:2005 provides for interchange of finger minutiae data between sensing, storage and matching systems.

ISO/IEC 19794-3:2006 – Biometric data interchange formats -- Part 3: Finger pattern spectral data, the finger pattern spectral data interchange format, specifies requirements for the representation of local or global spectral data derived from a fingerprint image. The format is designed to provide flexibility in the choice of spectral representation in that spectral components may be based on quantized co-sinusoidal triplets, Discrete Fourier Transformations or Gabor filters. The format also allows for a variable number of spectral components to be retained, which enables data representations in a form that is more compact than storage of the entire fingerprint image. ISO/IEC 19794-3:2006 provides example data records for each of the spectral representations.

ISO/IEC 19794-4:2005 – Biometric data interchange formats -- Part 4: Finger image data specifies a data record interchange format for storing, recording, and transmitting the information from one or more finger or palm image areas within an ISO/IEC 19785-1 CBEFF data structure. This can be used for the exchange and comparison of finger image data. It defines the content, format, and units of measurement for the exchange of finger image data that may be used in the verification or identification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, compressed or uncompressed images and vendor-specific information. This information is intended for interchange among organizations that rely on automated devices and systems for identification or verification purposes based on the information from finger image areas. Information compiled and formatted in accordance with ISO/IEC 19794-4:2005 can be recorded on machine-readable media or may be transmitted by data communication facilities.

ISO/IEC 19794-8:2006 – Biometric data interchange formats -- Part 8: Finger pattern skeletal data specifies the interchange format for the exchange of pattern-based skeletal fingerprint recognition data. The data format is generic, in that it may be applied and used in a wide range of application areas where automated fingerprint recognition is involved. The exchange format defined in ISO/IEC 19794-8:2006 describes all

characteristics of a fingerprint in a small data record. Thus it allows for the extraction of both spectral information (orientation, frequency, phase, etc.) and features (minutiae, core, ridge count, etc.). Transformations like translation and rotation can also be accommodated by the format defined herein. ISO/IEC 19794-8:2006 supports the proliferation of low-cost commercial fingerprint sensors with limited coverage, dynamic range, or resolution. Thus it defines a data record that can be used to store biometric information on a variety a storage media (including, but not limited to, portable devices and smart cards).

ISO/IEC 29109-2:2010 Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 -- Part 2: Finger minutiae data specifies elements of conformance testing methodology, test assertions, and test procedures as applicable to the biometric data interchange format standard relating to finger minutiae data (i.e. ISO/IEC 19794-2). It establishes tests of assertions of the structure of the finger minutiae data format as specified in ISO/IEC 19794-2:2005 (Type A Level 1 as defined in ISO/IEC 29109-1:2009), tests of assertions of internal consistency by checking the types of values that may be contained within each field (Type A Level 2 as defined in ISO/IEC 29109-1:2009), and tests of semantic assertions (Type A Level 3 as defined in ISO/IEC 29109-1:2009). ISO/IEC 29109-2:2010 does not establish tests of conformance of CBEFF structures embedding ISO/IEC 19794-2:2005 biometric data blocks (BDBs), tests of other characteristics of biometric products or other types of testing of biometric products (e.g. acceptance, performance, robustness, security), tests of conformance of systems that do not produce ISO/IEC 19794-2:2005 records, or tests for level 3 conformance testing.

ISO/IEC 29109-4:2010 - Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 -- Part 4: Finger image data specifies elements of conformance testing methodology, test assertions, and test procedures as applicable to ISO/IEC 19794-4. ISO/IEC 29109-4:2010 establishes test assertions of the structure of the finger image data format as specified in ISO/IEC 19794-4:2005 (Type A Level 1 as defined in ISO/IEC 29109-1:2009), test asssertions of internal consistency by checking the types of values that may be contained within each field (Type A Level 2 as defined in ISO/IEC 29109-1:2009), tests of semantic assertions (Type A Level 3 as defined in ISO/IEC 29109-1:2009). ISO/IEC 29109-4:2010 does not establish tests of conformance of CBEFF structures required by ISO/IEC 19794-4:2005, tests of other characteristics of biometric products or other types of testing of biometric products (e.g. acceptance, performance, robustness, security),

D.3 References

[12] Xie X., Su F., Cai A., "Ridge-Based Fingerprint Recognition," Book Series Lecture Notes in Computer Science, Publisher Springer Berlin / Heidelberg, ISSN 0302-9743 (Print) 1611-3349 (Online), Volume 3832/2005, Book Advances in Biometrics, DOI 10.1007/11608288, ISBN 978-3-540-31111-9, DOI 10.1007/1160828837, Pages 273-279

[13] Marana, A.N., Jain, A.K., "Ridge-Based Fingerprint Matching Using Hough Transform," *18th Brazilian Symposium on Computer Graphics and Image Processing*, vol., no., pp. 112- 119, 09-12 Oct. 2005

[14 Khalil M.S., Mohamad D., Khan M.K., Al-Nuzaili Q., "Fingerprint verification using statistical descriptors", Digital Signal Processing, Volume 20, Issue 4, July 2010, Pages 1264-1273

[15] Maio, D., Maltoni, D., "Direct gray-scale minutiae detection in fingerprints," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol.19, no.1, pp.27-40, Jan 1997

[16] Shapiro, L. G. and G. Stockman, *Computer Vision,* Prentice-Hall, New Jersey, 2001

[17] Jain, A.K., Hong L., Pankanti, S., Bolle, R., "An identity-authentication system using fingerprints," *Proceedings of the IEEE*, vol.85, no.9, pp.1365-1388, Sep 1997

Annex E   References and Bibliography

E.1   Articles Reviewed

Al-Assam, Hisham, Harin Sellahewa and Sabah Jassim. 2009. "A Lightweight Approach for Biometric Template Protection." SPIE Mobile Multimedia/Image Processing, Security, and Applications: 1-12.

Álvarez, F. Hernández, L. Hernández Encinas and C. Sánchez Ávila. 2009. "Biometric Fuzzy Extractor Scheme for Iris Templates."

Ang, Russell, Rei Safavi-Naini and Luke McAven. 2006. "Cancelable Key-Based Fingerprint Templates." ACISP (2005): 242-252.

Ballard, Lucas, Seny Kamara and Fabian Monrose. 2008. "Towards Practical Biometric Key Generation with Randomized Biometric Templates."

Barbosa, Manuel et al. 2008. "Secure Biometric Authentication With Improved Accuracy."

Barni, Mauro et al. 2010. "A Privacy-Compliant Fingerprint Recognition System Based on Homomorphic Encryption and Fingercode Templates."

Boult, T. E., W. J. Scheirer and R. Woodworth. 2007. "Revocable Fingerprint Biotokens: Accuracy and Security Analysis." IEEE CVPR.

Chen, B. and V. Chandran. 2007. "Biometric Based Cryptographic Key Generation from Faces." Proceedings of the 19th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications: 394-401.

Chen, Jin, Daniel Lopresti and Fabian Monrose. 2009. "Toward Resisting Forgery Attacks via Pseudo-Signatures." In Proceedings of the 10th International Conference on Document Analysis and Recognition: 51-55.

Chikkerur, Sharat et al. 2008. "Generating Registration-Free Cancelable Fingerprint Templates." IEEE.

Clancy, T. Charles, Negar Kiyavash and Dennis J. Lin. 2003. "Secure Smartcard-Based Fingerprint Authentication."

Costanzo, Christopher Ralph. 2004. "Biometric Cryptography: Key Generation Using Feature and Parametric Aggregation."

Dodis, Yevgeniy, et al. 2008. "Fuzzy Extractors: How to Generate Strong Keys From Biometrics and Other Noisy Data." SIAM Journal on Computing 38(1):97-139.

Farooq, Sergey Tulyakov Faisal, Praveer Mansukhani and Venu Govindaraju. 2007. "Symmetric Hash Functions for Secure Fingerprint Biometric Systems." State University of New York.

Freire-Santos, M., J. Fierrez-Aguilar and J. Ortega-Garcia. 2006. "Cryptographic Key Generation Using Handwritten Signature." Proceedings of SPIE 6202: 225-231.

Hao, Feng and C. W. Chan. 2002. "Private Key Generation From On-line Handwritten Signatures." Information Management & Computer Society 10(2): 159-164.

Hao, Feng, Ross Anderson and John Daugman. 2006. "Combining Cryptography with Biometrics Effectively." IEEE Transactions on Computers 55(9): 1081-1088.

Hirata, Shinji and Kenta Takahashi. 2009. "Cancelable Biometrics with Perfect Secrecy for Correlation-Based Matching." Lecture Notes in Computer Science, 5558: 868-878.

Huang, Yan et al. 2011. "Efficient Privacy-Preserving Biometric Identification." 18th Network and Distributed System Security Conference (NDSS 2011).

Jin, Zhe et al. 2009. "Secure Minutiae-Based Fingerprint Templates Using Random Triangle Hashing." LNCS 5857: 521-531.

Kanade, Sanjay, Dijana Petrovska-Delacrétaz and Bernadette Dorizzi. 2010. "Obtaining Cryptography Keys Using Feature Level Fusion of Iris and Face Biometrics for Secure User Authentication." IEEE.

Li, Qiming, Yagiz Sutcu and Nasir Memon. 2006. "Secure Sketch for Biometric Templates." Asiascrypt.

Linnartz, Jean-Paul and Pim Tuyls. 2003. "New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates." AVBPA, LNCS.

Maiorana, E. et al. 2008. "Template Protection for HMM-Based Signature Recognition." Proceedings on the 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems: 1-6.

Merkle, Johannes et al. 2010. "Performance of the Fuzzy Vault for Multiple Fingerprints. Gesellschaft für Informatik.

Monrose, Fabian, et al. 2001. "Cryptographic Key Generation from Voice." Proceedings of the 2001 IEEE Symposium on Security and Privacy: 12-25.

Monrose, Fabian, Michael K. Reiter and Susanne Wetzel. 2001. "Password Hardening Based on Keystroke Dynamics." International Journal of Information Security 1(2): 69-83.

Nagar, Abhishek, Karthik Nandakumar, and Anil K. Jain. 2009. "A Hybrid Biometric Cryptosystem for Securing Fingerprint Templates." Pattern Recognition.

Nagar, Abhishek, Shantanu Rane and Anthony Vetro. 2010. "Alignment and Bit Extraction for Secure Fingerprint Biometrics." Mitsubishi Electric Research Laboratories.

Nandakumar, Karthik, Abhishek Nagar and Anil K. Jain. 2007. "Hardening Fingerprint Fuzzy Vault Using Password." Proceedings of the 2nd International Conference on Biometrics: 109-124.
Nandakumar, Karthik and Anil K. Jain. 2008. "Multibiometric Template Security Using Fuzzy Vault."

Ŏrencik, C. et al. 2008. "Improved Fuzzy Vault Scheme for Fingerprint Verification."

Ouda, Osama, Norimichi Tsumura and Toshiya Nakaguchi. 2010. "BioEncoding: A Reliable Tokenless Cancelable Biometrics Scheme for Protecting IrisCodes." The Institute of Electronics, Information and Communication Engineers.

Scheirer, W. and T. E. Boult. 2008. "Bio-Cryptographic Protocols with Bipartite Biotokens."

. 2009. "Bipartite Biotokens: Definition, Implementation, and Analysis."

Shi, Jinyang et al. 2008. "Biomapping: Privacy Trustworthiness Biometrics Using Noninvertible and Discriminable Constructions." Pattern Recognition: 1-4.

Soutar, et al. 1999. "Biometric Encryption."

Sutcu, Yagiz, Qiming Li and Nasir Memon. 2007. "How to Protect Biometric Templates."

Sutcu, Yagiz et al. 2008. "Feature Extraction for a Slepian-Wolf Biometric System Using LDPC Codes." Mitsubishi Electric Research Laboratories.

Takahashi, Kenta and Shinji Hirata. 2009. "Generating Provably Secure Cancelable Fingerprint Templates Based on Correlation-Invariant Random Filtering." IEEE.

Teoh, Andrew Beng Jin and Chong Tze Yuang. 2007. "Cancellable Biometrics Realization with Multispace Random Projections." IEEE Transactions on Systems 37(5): 1096-1106.

Teoh, Andrew Beng, C. I. David Ngo and A. Goh. 2004. "BioHashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number." Pattern Recognition 37(11): 2245-2255.

Tuyls, Pim et al. 2004. "Privacy Protected Biometric Templates: Acoustic Ear Identification." SPIE Defence and Security Symposium.

Uludag, Umut and Anil Jain. 2006. "Securing Fingerprint Template: Fuzzy Vault with Helper Data." Proceedings of the Computer Vision and Pattern Recognition Workshops (CVPR '06).

Van der Veen, Michiel, Tom Kevenaar and Geert-Jan Schrijen. 2006. "Face Biometrics with Renewable Templates." SPIE 6072.

Vielhauer, Claus, Ralf Steinmetz and Astrid Mayerhöfer. 2002. "Biometric Hash Based on Statistical Features of Online Signatures." Proceedings of the IEEE International Conference on Pattern Recognition (1): 123-126.

Yang, Bian et al. 2010. "Dynamic Random Projection for Biometric Template Protection." 4th IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS).

Ye, Shuiming et al. 2009. "Anonymous Biometric Access Control." EURASIP Journal on Information Security.

Zheng, Gang, Wanqing Li and Ce Zhan. 2006. "Cryptographic Key Generation from Biometric Data Using Lattice Mapping." Pattern Recognition 14: 513-516.

E.2 Patents Reviewed

Akkermans, Antonius Hermanus Maria et al. 2007. "Biometric Template Protection and Feature Handling." U.S. Patent Application 11/570,044.

Bjorn, Vance. 2000. "Cryptographic Key Generation Using Biometric Data." U.S. Patent 6,035,398.

Bolle, Rudolf Maarten et al. 2009. "Anonymous and Revocable Fingerprint Recognition." U.S. Patent Application 12/187,705.

Bolle, Rudolf Maarten, Jonathan H. Connell and Nalini K. Ratha. 2004. "System and Method for Distorting a Biometric for Transactions with Enhanced Security and Privacy." U.S. Patent 6,836,554.

Bolle, Rudolf M., Nalini K. Ratha and Jonathan H. Connell. 2009a. "Method, Apparatus and Computer Program Product Implementing Anonymous Biometric Matching." U.S. Patent Application 11/939,135.

Bolle, Rudolf Maarten, et al. 2009b. "Method and Apparatus for Generation of Cancelable Fingerprint Template." U.S. Patent Application 11/971,634.

Chang, Yao-Jen, Tsu-Han Chen and Wen-De Zhung. 2010. "Biometrics-Based Cryptographic Key Generation System and Method." U.S. Patent 7,804,956.

Connell, Jonathan Hudson and Nalini Kanta Ratha. 2009. "Method and Apparatus for Generation of Cancelable Face Template." U.S. Patent Application 11/971,643.

Davida, George I. and Yair Frankel. 2010. "System and Method for Authenticated and Privacy Preserving Biometric

Identification Systems." U.S. Patent 7,711,152.

Davida, George I., Yair Frankel and Brian J. Matt. 1998. "On Enabling Secure Applications Through Off-line Biometric Identification."

Draper, Stark C. et al. 2010. "Biometric Based User Authentication and Data Encryption." U.S. Patent 7,779,268.

Kevenaar, Thomas Andreas Maria et al. 2007. "Architectures for Privacy Protection of Biometric Templates." U.S. Patent Application 11/570,046.

. 2010. "Defining Classification Thresholds in Template Protection Systems." U.S. Patent Application 12/808,579.

Martinian, Emin and Anthony Vetro. 2006. "Biometric Based User Authentication With Syndrome Codes." U.S. Patent Application 11/006,308.

Takahashi, Kenta et al. 2008. "Method, System and Program for Authenticating a User by Biometric Information." U.S. Patent Application 11/691,575.

Tomko, George J., Colin Soutar and Gregory J. Schmidt. 1998. "Fingerprint Controlled Public Key Cryptographic System." U.S. Patent 5,832,091.

Tomko, George J. and Alexei Stoianov. 1998. "Method and Apparatus for Securely Handling a Personal Identification Number or Cryptographic Key Using Biometric Techniques." U.S. Patent 5,712,912.

Van Someren, Nicholas Benedict. 2003. "Biometric Key Generation for Secure Storage." U.S. Patent Application 10/115,594.

E.3 Related Articles

Adler, Andy. 2007. "Vulnerabilities in Biometric Encryption Systems."

Ballard, Lucas, Seny Kamara and Michael K. Reiter. 2008. "The Practical Subtleties of Biometric Key Generation." Proceedings of the 17th USENIX Security Symposium: 61-74.

Bringer, Julien et al. 2007. "An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication." The 12th Australasian Conference on Information Security and Privacy.

Chang, W., R. Chen and F. W. Teo, 2006, "Finding the Original Point Set Hidden Among Chaff," in Proceedings of the ACM Symposium on Information, Computer and Communication Secrecy.

Cheung, King-Hong et al. 2005. "An Analysis on Accuracy of Cancelable Biometrics Based on BioHashing."

Ignatenko, Tanya, and Frans M. J. Willems. 2009. "Biometric Systems: Privacy and Secrecy Aspects." IEEE Transactions on Information Forensics and Security 4(4):956-973.

Jain, Anil K., Karthik Nandakumar and Abhishek Nagar. 2008. "Biometric Template Security."

Johnson, W.B. and J. Lindenstrauss. 1984. "Extension of Lipschizt Mapping into a Hilbert Space," in Proceedings of the Conference on Modern Analysis and Probability: 189-206.

Juels, Ari and Madhu Sudan. 2002. "A Fuzzy Vault Scheme." International Symposium on Information Theory.

Juels, Ari and Martin Wattenberg. 1999. "A Fuzzy Commitment Scheme." Proceedings of the 6th ACM Conference on Computer and Communication Security: 28-36.

Kholmatov, Alisher. 2008. "Privacy Protecting Biometric Authentication System."

Kong, Adams et al. 2006. "An Analysis of BioHashing and Its Variants."

Lalithamani, N. and K. P. Soman. 2009. "Irrevocable Cryptographic Key Generation from Cancelable Fingerprint Templates: An Enhanced and Effective Scheme." European Journal of Scientific Research 31(3): 372-387.

Mihăilescu, Preda. 2007. "The Fuzzy Vault for Fingerprint is Vulnerable to Brute Force Attack."

Nagar, Abhishek, Shantanu Rane and Anthony Vetro. 2010. "Privacy and Security of Features Extracted from Minutiae Aggregates." Mitsubishi Electric Research Laboratories.

Paillier, Pascal. 1999. "Public-Key Cryptosystem Based on Composite Degree Residuosity Classes." Lecture Notes in Computer Science 1592: 223-238.

Poon, Hoi Ting and Ali Miri. 2009. "A Collusion Attack on the Fuzzy Vault Scheme." ISC International Journal of Information Security: 27-34.

Ratha, N. K., J. H. Connell and R. M. Bolle. 2001. "Enhancing Security and Privacy in Biometrics-Based Authentication Systems." IBM Systems Journal 40(3): 614-634.

Scheirer, Walter J. and Terrance E. Boult. 2008. "Cracking Fuzzy Vaults and Biometric Encryption."

Teoh, Andrew B. J., Yip Wai Kuan and Sangyoun Lee. 2008. "Cancellable Biometrics and Annotations on BioHash." Pattern Recognition 41(2008): 2034-2044.

Uludag, Umut. 2008. "Secure Biometric Systems."

Uludag, Umut et al. 2004. "Biometric Cryptosystems: Issues and Challenges." Proceedings of the IEEE 92 (6): 948-960.

Wang, Yongjin and Konstantinos Plataniotis. 2010. "An Analysis of Random Projection for Changeable and Privacy-Preserving Biometric Verification." IEEE Transactions on Systems, Man, and Cybernetics 40(5): 1280-1293.

Annex F   Summary of Literature on PET Evaluation Results

Figure 79 lists the results of each empirical study reviewed, sorted in ascending order by false rejection rate (FRR). FRR is the focus of this table because it generally represents the usability of the proposed method. Results are highlighted where a target of 1% FRR at 0.1% FRR was achieved. Some tests ran multiple trials and obtained multiple results. In such cases, optimal results are listed. The other metrics are listed at the value that was needed to achieve that level of FRR. In many cases, FRR and FAR were derived from a reported equal error rate (EER).

Article	Method	Modality	Mode	n =	FRR	FAR	Bits
Teoh et al. (2004)	Multifactor	Fingerprint	1:1	600	0.0%	0.0%	80
Hirata and Takahashi (2009)	Transform	Vein	1:1	102	0.0%	0.0%	-
Chikkerur et al. (2008)	Projection	Fingerprint	1:1	188	0.0%	0.1%	-
Kanade et al. (2010)	Multifactor	Multimodal	1:1	1,750	0.11%	0.0%	210
Al-Assam et al. (2009)	Projection	Face	1:1	80	0.2%	0.2%	-
Jin et al. (2009)	Aggregation	Fingerprint	1:1	800	0.2%	0.2%	4800
Van der Veen et al. (2006)	Fuzzy	Face	1:1	96	0.25%	0.25%	-
Hao et al. (2006)	Multifactor	Iris	1:1	700	0.47%	0.0%	140
Linnartz and Tuyls (2003)	Fuzzy	Ear	1:1	360	0.6%	0.05%	343
Yang et al. (2010)	Projection	Fingerprint	1:1	700	0.6%	0.1%	144
Chen et al. (2009)	Parametric	Pseudo-sig	1:1	350	1.0%	1.0%	-
Boult et al. (2007)	Biotoken	Fingerprint	1:1	2,800	1.2%	1.2%	-
Shi et al. (2008)	Transform	Fingerprint	1:1	800	1.35%	1.35%	-
Õrencik et al. (2008)	Fuzzy	Fingerprint	1:1	360	1.5%	0.0%	-
Zheng et al. (2006)	Fuzzy	Iris	1:1	150	1.5%	1.5%	-
Nandakumar and Jain (2008)	Fuzzy	Multimodal	1:1	-	1.8%	0.0%	224
Ang et al. (2005)	Transform	Fingerprint	1:1	800	2.0%	2.0%	-
Nagar et al. (2010)	Aggregation	Fingerprint	1:1	-	2.0%	2.0%	-
Ouda et al. (2010)	Projection	Iris	1:1	80	2.2%	2.2%	450
Sutcu et al. (2008)	Aggregation	Fingerprint	1:1	1,035	2.7%	2.7%	30
Scheirer and Boult (2009)	Biotoken	Fingerprint	1:1	-	3.0%	0.0%	256
Sutcu et al. (2007)	Fuzzy	Face	1:1	1,216	3.8%	0.7%	108
Ye et al. (2009)	Homomorphic	Iris	1:N	1,948	4.0%	0.0%	1024
Monrose et al. (2001b)	Multifactor	Voice	1:1	250	5.0%	-	60
Nagar et al. (2009)	Fuzzy	Fingerprint	1:1	-	5.0%	0.01%	-
Takahashi and Hirata (2009)	Transform	Fingerprint	1:1	181	5.0%	0.2%	-
Barni et al. (2010)	Homomorphic	Fingerprint	1:N	408	6.5%	6.5%	128
Vielhauer et al. (2002)	Parametric	Signature	1:1	-	7.05%	0.0%	-
Nandakumar et al. (2007)	Fuzzy	Fingerprint	1:1	800	10.0%	0.0%	70
Maiorana et al. (2008)	Transform	Signature	1:1	16,500	10.29%	10.29%	-
Álvarez et al. (2009)	Fuzzy	Iris	1:1	175	11.1%	0.67%	-
Uludag and Jain (2006)	Fuzzy	Fingerprint	1:1	800	15.5%	0.0%	-
Ballard et al. (2008)	Multifactor	-	1:1	-	17.7%	17.7%	-
Teoh et al. (2007)	Projection	Face	1:1	600	18.1%	18.1%	127
Monrose et al. (2001a)	Multifactor	Keystroke	1:1	188	22.9%	-	16
Hao and Chan. (2002)	Parametric	Signature	1:1	750	28.0%	1.2%	40
Clancy et al. (2003)	Fuzzy	Fingerprint	1:1	-	30.0%	0.0%	-
Freire-Santos et al. (2006)	Fuzzy	Signature	1:1	16,500	57.3%	0.32%	-
Chen and Chandran (2007)	Transform	Face (3D)	1:1	-	66.0%	0.26%	64

Figure 79: Summary of PET Test Results

Annex G   References: Iris Recognition Accuracy with Variable-Quality Datasets

[1] J. Daugman, "Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons," *Proceedings of the IEEE,* vol. 94, no. 11, pp. 1927-1935, 2006.

[2] J. Daugman, "How iris recognition works," *Circuits and Systems for Video Technology, IEEE Transactions on,* vol. 14, no. 1, pp. 21-30, 2004.

[3] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 15, no. 11, pp. 1148-1161, 1993.

[4] R. Wildes, "Iris recognition: an emerging biometric technology," *Proceedings of the IEEE,* vol. 85, no. 9, pp. 1348-1363, 2002.

[5] J. R. Matey, O. Naroditsky, K. Hanna *et al.*, "Iris on the Move: Acquisition of Images for Iris Recognition in Less Constrained Environments," *Proceedings of the IEEE,* vol. 94, no. 11, pp. 1936-1947, 2006.

[6] C. Fancourt, L. Bogoni, K. Hanna *et al.*, "Iris recognition at a distance," *AVBPA,* vol. 3546, pp. 1-13, 2005, 2005.

[7] R. Narayanswamy, G. E. Johnson, P. E. X. Silveira *et al.*, "Extending the imaging volume for biometric iris recognition," *Appl. Opt.,* vol. 44, pp. 701-712, 2005.

[8] E. Arvacheh, and H. Tizhoosh, "Iris segmentation: Detecting pupil, limbus and eyelids," pp. 2453-2456, 2007.

[9] C.-T. Chou, S.-W. Shih, W.-S. Chen *et al.*, "Non-Orthogonal View Iris Recognition System," *Circuits and Systems for Video Technology, IEEE Transactions on,* vol. 20, no. 3, pp. 417-430, 2010.

[10] J. Zuo, and N. A. Schmid, "On a Methodology for Robust Segmentation of Nonideal Iris Images," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on,* vol. 40, no. 3, pp. 703-718, 2010.

[11] H. Proenca, "Iris Recognition: On the Segmentation of Degraded Images Acquired in the Visible Wavelength," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 32, no. 8, pp. 1502-1516, 2010.

[12] H. Proenca, and L. A. Alexandre, "Iris segmentation methodology for non-cooperative recognition," *Vision, Image and Signal Processing, IEE Proceedings -,* vol. 153, no. 2, pp. 199-205, 2006.

[13] H. Proenca, and L. A. Alexandre, "Toward Noncooperative Iris Recognition: A Classification Approach Using Multiple Signatures," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 29, no. 4, pp. 607-612, 2007.

[14] R. N. Rakvic, B. J. Ulis, R. P. Broussard *et al.*, "Parallelizing Iris Recognition," *Information Forensics and Security, IEEE Transactions on,* vol. 4, no. 4, pp. 812-823, 2009.

[15] S. Shah, and A. Ross, "Iris Segmentation Using Geodesic Active Contours," *Information Forensics and Security, IEEE Transactions on,* vol. 4, no. 4, pp. 824-836, 2009.

[16] M. Vatsa, R. Singh, and A. Noore, "Improving Iris Recognition Performance Using Segmentation, Quality Enhancement, Match Score Fusion, and Indexing," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on,* vol. 38, no. 4, pp. 1021-1035, 2008.

[17] Z. He, T. Tan, Z. Sun *et al.*, "Toward Accurate and Fast Iris Segmentation for Iris Biometrics," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 31, no. 9, pp. 1670-1684, 2009.

[18] Z. Zhou, Y. Du, and C. Belcher, "Transforming Traditional Iris Recognition Systems to Work in Nonideal Situations," *Industrial Electronics, IEEE Transactions on,* vol. 56, no. 8, pp. 3203-3213, 2009.

[19] L. Ma, Y. Wang, and T. Tan, "Iris recognition using circular symmetric filters," *Proceedings of the 16th International Conference on Pattern Recognition,* vol. 2, pp. 414-417, 2002.

[20] J. Huang, L. Ma, Y. Wang *et al.*, "Iris recognition based on local orientation description," *Proc. 6th Asian Conf. Computer Vision,* vol. 2, pp. 954-959, 2004.

[21] Y. Du, R. Ives, D. Etter *et al.*, "Use of one-dimensional iris signatures to rank iris pattern similarities," *Optical Engineering,* vol. 45, pp. 037201, 2006.

[22] C. Tisse, L. Martin, L. Torres *et al.*, "Person identification technique using human iris recognition," pp. 294-

299, 2002.

[23] S. A. C. Schuckers, N. A. Schmid, A. Abhyankar *et al.*, "On Techniques for Angle Compensation in Nonideal Iris Recognition," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on,* vol. 37, no. 5, pp. 1176-1190, 2007.

[24] Y. Du, E. Arslanturk, Z. Zhou *et al.*, "Video-based Non-cooperative Iris Image Segmentation," *IEEE Trans. On Systems, Man, and Cybernetics, Part B,* vol. 41, no. 1, pp. 64-74, 2011.

[25] J. Daugman, "New Methods in Iris Recognition," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on,* vol. 37, no. 5, pp. 1167-1175, 2007.

[26] K. W. Bowyer, K. Hollingsworth, and P. J. Flynn, "Image Understanding for Iris Biometrics: A Survey," *Computer Vision and Image Understanding,* vol. 110, pp. 281-307, 2008.

[27] Y. Du, "Review of Iris Recognition: Cameras, Systems, and Their Applications," *Sensor Review,* vol. 26, no. 1, pp. 66-69, 2006.

[28] L. Masek, "Recognition of human iris patterns for biometric identification," *Bachelor of Engineering degree, School of Computer Science and Software Engineering, University of Wester Austrialia*, 2003.

[29] K. P. Hollingsworth, K. W. Bowyer, and P. J. Flynn, "The Best Bits in an Iris Code," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 31, no. 6, pp. 964-973, 2009.

[30] M. Li, T. Tan, Y. Wang *et al.*, "Personal identification based on iris texture analysis," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 25, no. 12, pp. 1519-1533, 2003.

[31] D. Monro, S. Rakshit, and D. Zhang, "DCT-based iris recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 586-595, 2007.

[32] K. Miyazawa, K. Ito, T. Aoki *et al.*, "An effective approach for iris recognition using phase-based image matching," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 30, no. 10, pp. 1741-1756, 2008.

[33] R. Zhu, J. Yang, and R. Wu, "Iris Recognition Based on Local Feature Point Matching," *Communications and Information Technologies, International Symposium on*, pp. 451-454, 2006.

[34] E. Krichen, S. Garcia-Salicetti, and B. Dorizzi, "A new phase-correlation-based Iris matching for degraded images," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on,* vol. 39, no. 4, pp. 924-934, 2009.

[35] C. Belcher, and Y. Du, "Region-based sift approach to iris recognition," *Optics and Lasers in Engineering,* vol. 47, no. 1, pp. 139-147, 2009.

[36] J. Thornton, M. Savvides, and V. Kumar, "A Bayesian Approach to Deformed Pattern Matching of Iris Images," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 29, no. 4, pp. 596-606, 2007.

[37] N. Sudha, N. B. Puhan, H. Xia *et al.*, "Iris recognition on edge maps," *Computer Vision, IET,* vol. 3, no. 1, pp. 1-7, 2009.

[38] V. Velisavljevic, "Low-Complexity Iris Coding and Recognition Based on Directionlets," *Information Forensics and Security, IEEE Transactions on,* vol. 4, no. 3, pp. 410-417, 2009.

[39] H. Proença, and L. A. Alexandre, "UBIRIS: A noisy iris image database," *13th International Conference on Image Analysis and Processing,* vol. LNCS 3617, pp. 970-977, 2005.

[40] Y. Du, B. Craig, and Z. Zhou, "Scale Invariant Gabor Descriptor-based Noncooperative Iris Recognition," *EURASIP Journal on Advances in Signal Processing,* vol. 2010, pp. 936512:1-13, 2010.

[41] C. Boyce, A. Ross, M. Monaco *et al.*, "Multispectral Iris Analysis: A Preliminary Study," *Computer Vision and Pattern Recognition Workshop On Biometrics*, 2006.

[42] A. Ross, R. Pasula, and L. Hornak, "Exploring multispectral Iris recognition beyond 900nm," *Proceedings of the 3rd IEEE international conference on Biometrics: Theory, applications and systems*, 2009.

[43] A. Abhyankar, and S. Schuckers, "Iris quality assessment and bi-orthogonal wavelet based encoding for recognition," *Pattern Recognition,* vol. 42, no. 9, pp. 1878-1894, 2009.

[44] C. Belcher, and Y. Du, "A Selective Feature Information Approach for Iris Image-Quality Measure," *Information Forensics and Security, IEEE Transactions on,* vol. 3, no. 3, pp. 572-577, 2008.

[45] Y. Chen, S. Dass, and A. Jain, "Localized iris image quality using 2-D wavelets," *Advances in Biometrics*, pp. 373-381, 2005.

[46] Y. Du, C. Belcher, Z. Zhou *et al.*, "Feature correlation evaluation approach for iris feature quality measure," *Signal Processing,* vol. 90, no. 4, pp. 1176-1187, 2010.

[47] M. Gamassi, M. Lazzaroni, M. Misino *et al.*, "Quality assessment of biometric systems: a comprehensive perspective based on accuracy and performance measurement," *Instrumentation and Measurement, IEEE Transactions on,* vol. 54, no. 4, pp. 1489-1496, 2005.

[48] N. D. Kalka, J. Zuo, N. A. Schmid *et al.*, "Estimating and Fusing Quality Factors for Iris Biometric Images," *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on,* vol. 40, no. 3, pp. 509-524, 2010.

[49] N. Poh, T. Bourlai, J. Kittler *et al.*, "Benchmarking Quality-Dependent and Cost-Sensitive Score-Level Multimodal Biometric Fusion Algorithms," *Information Forensics and Security, IEEE Transactions on,* vol. 4, no. 4, pp. 849-866, 2009.

[50] N. A. Schmid, and F. Nicolo, "On Empirical Recognition Capacity of Biometric Systems Under Global PCA and ICA Encoding," *Information Forensics and Security, IEEE Transactions on,* vol. 3, no. 3, pp. 512-528, 2008.

[51] G. C. Stone, "Partial discharge diagnostics and electrical equipment insulation condition assessment," *Dielectrics and Electrical Insulation, IEEE Transactions on,* vol. 12, no. 5, pp. 891-904, 2005.

[52] G. O. Williams, "Iris recognition technology," *Aerospace and Electronic Systems Magazine, IEEE,* vol. 12, no. 4, pp. 23-29, 1997.

[53] H. Xiaofu, Y. Jingqi, C. Guangyu *et al.*, "Contactless Autofeedback Iris Capture Design," *Instrumentation and Measurement, IEEE Transactions on,* vol. 57, no. 7, pp. 1369-1375, 2008.

[54] X. Zhu, Y. Liu, X. Ming *et al.*, "A Quality Evaluation Method of Iris Images Sequence Based on Wavelet Coefficients in Region of Interest," *CIT '04 Proceedings of the The Fourth International Conference on Computer and Information Technology*, pp. 24-27, 2004.

[55] F. Scotti, and V. Piuri, "Adaptive Reflection Detection and Location in Iris Biometric Images by Using Computational Intelligence Techniques," *Instrumentation and Measurement, IEEE Transactions on,* vol. 59, no. 7, pp. 1825-1833, 2010.

[56] G. Zhang, and M. Salganicoff, "Method of measuring the focus of close-up images of eyes," Google Patents, 1999.

[57] S. Anderson, and J. Morris, "Transitions in the polarimetric radar scattering properties of the sea surface," *Radar, Sonar & Navigation, IET,* vol. 4, no. 2, pp. 251-264, 2010.

[58] "OKI Introduces Japan's First Iris Recognition for Camera-equipped Mobile Phones and PDAs Enables user-recognition for mobile terminals using general optical cameras," http://www.oki.com/. 2011.

[59] "Hoyos Consumer Products," http://www.hoyosgroup.com/. 2010.

[60] "VeriEye Iris Recognition Technology," http://www.neurotechnology.com/. 2011.

[61] "AOPTIX Technologies: InSight VM," http://www.aoptix.com/. 2010.

[62] Y. Du, and C.-I. Chang, "3D Combinational Curves for Accuracy and Performance Analysis of Positive Biometrics Identification," *Optics and Lasers in Engineering,* vol. 46, pp. 477-490, 2008.

[63] http://iris.nist.gov/ice/. January 2011.

[64] "CASIA iris image database," http://www.sinobiometrics.com. January 2011.

[65] A. Ross, S. Crihalmeanu, L. Hornak *et al.*, "A centralized web-enabled multimodal biometric database," *Proc. 2004 Biometric Consortium Conf*, 2004.

[66] NIST. "Multiple Biometric Grand Challenge," http://face.nist.gov/mbgc/. January 2011.

[67] R. W. Ives, D. A. Bishop, Y. Du *et al.*, "Iris Recognition: The Consequence of Image Compression," *EURASIP Journal on Advances in Signal Processing,* vol. 2010, pp. 680845:1-9, 2010.

[68] P. J. Phillips, K. W. Bowyer, P. J. Flynn *et al.*, "The Iris Challenge Evaluation 2005," *Biometrics: Theory,*

Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on, pp. 1-8, 2008.

[69] M. D. Adams. "The JasPer Project Home Page," http://www.ece.uvic.ca/~mdadams/jasper/. 2010.

[70] Y. Du, C.-I. Chang, H. Ren *et al.*, "A New Hyperspectral Discrimination Measure for Spectral Similarity," *Optical Engineering,* vol. 43(8), pp. 1777-1786, 2004.

[71] J. Daugman, and C. Downing, "Effect of Severe Image Compression on Iris Recognition Performance," *IEEE Transactions on Information Forensices and Security,* vol. 3, no. 1, pp. 52-61, 2008.

[72] S. E. Baker, A. Hentz, K. W. Bowyer *et al.*, "Degradation of Iris Recognition Performance Due to Non-Cosmetic Prescription Contact Lenses," *Computer Vision and Image Understanding* vol. 114, pp. 1030-1044, 2010.

[73] X. Liu, K. W. Bowyer, and P. J. Flynn, "Experiments with an improved iris segmentation algorithm," *Automatic Identification Advanced Technologies, 2005. Fourth IEEE Workshop on*, pp. 118-123, 2005.

[74] T. M. Aslam, S. Z. Tan, and B. Dhillon, "Iris recognition in the presence of ocular disease," *Journal of The Royal Society*, pp. 1-5, 2009.

[75] H. Proenca, S. Filipe, R. Santos *et al.*, "The UBIRIS.v2: A Database of Visible Wavelength Iris Images Captured On-the-Move and At-a-Distance," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 32, no. 8, pp. 1529-1535, 2010.

[76] N. Thomas, Y. Du, and Z. Zhou, "A new approach for sclera vein recognition," *SPIE Symposium on Defense, Security + Sensing,* vol. 7708, pp. 770805:1-10, 2010.

[77] Z. Zhou, Y. Du, N. Thomas *et al.*, "Multimodal eye recognition," *SPIE Symposium on Defense, Security and Sensing,* vol. 7708, pp. 770806:1-10, 2010.

DOCUMENT CONTROL DATA
(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR Defence R&D Canada – CSS 222 Nepean St Ottawa, Ontario K1A 0K2	2. SECURITY CLASSIFICATION UNCLASSIFIED

3. TITLE Biometric Data Safeguarding Technologies Analysis and Best Practices

4. AUTHORS Raj Nanavati International Biometric Group

5. DATE OF PUBLICATION December 2011	6a. NO. OF PAGES 177	6b. NO. OF REFS 94

7. DESCRIPTIVE NOTES Contract Report

8. SPONSORING ACTIVITY Defence R&D Canada – CSS 222 Nepean St Ottawa, Ontario K1A 0K2

9a. PROJECT OR GRANT NO. PSTP 02-0351BIO	9b. CONTRACT NO.

10a. ORIGINATOR'S DOCUMENT NUMBER DRDC CSS CR 2011-29	10b. OTHER DOCUMENT NO(s).

11. DOCUMENT AVAILABILITY UNCLASSIFIED

12. DOCUMENT ANNOUNCEMENT   UNLIMITED

13. ABSTRACT

This document is the Study Report for PSTP 02-0351BIO, Biometric Data Safeguarding Technologies Analysis and Best Practices. One of the main goals of the Public Security Technical Program (PSTP) Biometrics Community of Practice is to evaluate, analyze, and implement biometric technologies that enhance national capabilities in access control, identity verification, and e-Commerce security in a manner that is consistent with Canadian laws and acts. This is done in collaboration with the appropriate Government of Canada agencies and departments responsible for national security, border control and security, and law enforcement and immigration.

The rapid progress of biometrics technology in the last few years and the ease with which biometrics data can be acquired has resulted in the accumulation of large varying databases of biometrics information. This trend will continue in the future, with databases growing at an ever-increasing rate. The purpose of the Study is to examine some of the issues surrounding the sharing and safeguarding of biometric data in the Canadian Public Security context writ large. Throughout the study, the modality focus will be on iris biometrics (prime focus) and fingerprints (secondary).

This document presents methodologies and results from scientific studies that identify and evaluate biometric technologies with respect to their ability to be used securely (in terms of safeguarding biometric databases). These new biometric technologies and associated data safeguarding capabilities must be consistent with the Government of Canada's dual prosperity and security mandates, and must consider legal, ethical, cultural, and privacy issues.

Le présent document constitue le Rapport d'étude PSTP 02-0351BIO, Analyse et meilleures pratiques relatives aux technologies de protection des données biométriques. L'un des principaux objectifs du Programme technique de sécurité publique (PTSP) de la Communauté de praticiens en biométrie est d'évaluer, d'analyser et de mettre en application des technologies biométriques qui améliorent les capacités du pays en matière de contrôle de l'accès, de la vérification de l'identité et de la sécurité de commerce électronique tout en respectant les lois et les actes canadiens. Ces mesures sont prises en collaboration avec les agences et ministères du gouvernement canadien responsables de la sécurité nationale, du contrôle frontalier et de sécurité à la frontière, avec la police et les services d'immigration.

L'évolution rapide des technologies biométriques des dernières années et la facilité avec laquelle les données biométriques peuvent être acquises ont mené à une accumulation de vastes bases de renseignements biométriques divers. Cette tendance se maintiendra étant donné le rythme constant avec lequel les bases de données sont alimentées. L'objectif de la présente étude est d'examiner certaines questions relatives au partage et à la protection des données biométriques dans le contexte de la sécurité publique au Canada. Au cours de l'étude, l'accent sera placé sur les données biométriques de l'iris (point principal) et les empreintes digitales (point secondaire).

Le présent document introduit des méthodologies et les résultats d'études scientifiques qui identifient et évaluent les technologies biométriques sur leur capacité à être utilisées de manière sécurisée (en terme de protection des bases de données biométriques). Ces nouvelles technologies biométriques et les capacités de protection de données connexes doivent être conformes aux mandats de prospérité et de sécurité du gouvernement canadien et doivent prendre en considération les questions relatives au droit, à l'éthique, à la culture et à la protection des renseignements personnels.

---

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS
   Biometric Data; e-Commerce Security; Border Control and Security